ADMINISTRATION GUIDE

Cisco Small Business

ISA500 Series Integrated Security Appliances
(ISA550, ISA550W, ISA570, ISA570W)

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.
78-20776-03

Federal Communication Commission Interference Statement

(For ISA570 and ISA570W)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

(For ISA550 and ISA550W)

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement: (For ISA550W and ISA570W)

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Industry Canada statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

IMPORTANT NOTE:

Canada Radiation Exposure Statement: (For ISA550W and ISA570W)

This equipment complies with Canada radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

NOTE IMPORTANTE: (Pour l'utilisation de dispositifs mobiles)

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

This device has been designed to operate with an antenna having a maximum gain of 1.8 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

(Le manuel d'utilisation de dispositifs émetteurs équipés d'antennes amovibles doit contenir les informations suivantes dans un endroit bien en vue:)

Ce dispositif a été conçu pour fonctionner avec une antenne ayant un gain maximal de 1.8 dBi. Une antenne à gain plus élevé est strictement interdite par les règlements d'Industrie Canada. L'impédance d'antenne requise est de 50 ohms.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peutfonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pourl'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectriqueà l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que lapuissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire àl'établissement d'une communication satisfaisante.

UL/CB

Rack Mount Instructions - The following or similar rack-mount instructions are included with the installation instructions:

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) 40 degree C specified by the manufacturer.

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Contents

Chapter 1: Getting Started 19

Introduction 20
Product Overview 21
Front Panel 21
Back Panel 23
Getting Started with the Configuration Utility 25
Logging in to the Configuration Utility 26
Navigating Through the Configuration Utility 27
Using the Help System 28
Configuration Utility Icons 28
Factory Default Settings 30
Default Settings of Key Features 30
Restoring the Factory Default Settings 31
Performing Basic Configuration Tasks 32
Changing the Default Administrator Password 32
Upgrading your Firmware After your First Login 33
Backing Up Your Configuration 34

Chapter 2: Configuration Wizards 35

Using the Setup Wizard for the Initial Configuration 36
Starting the Setup Wizard 37
Configuring Cisco.com Account Credentials 37
Enabling Firmware Upgrade 38
Validating Security License 39
Enabling Bonjour and CDP Discovery Protocols 39
Configuring Remote Administration 40
Configuring Physical Ports 41
Configuring the Primary WAN 42
Configuring the Secondary WAN 42
Configuring WAN Redundancy 42
Configuring Default LAN Settings 43
Configuring DMZ 44

Configuring DMZ Services 45
Configuring Wireless Radio Settings 47
Configuring Intranet WLAN Access 48
Configure Security Services 49
Viewing Configuration Summary 50
Using the Dual WAN Wizard to Configure WAN Redundancy Settings 51
Starting the Dual WAN Wizard 51
Configuring a Configurable Port as a Secondary WAN Port 51
Configuring the Primary WAN 52
Configuring the Secondary WAN 52
Configuring WAN Redundancy 52
Configuring Network Failure Detection 53
Viewing Configuration Summary 54
Using the Remote Access VPN Wizard 54
Using the Remote Access VPN Wizard for IPsec Remote Access 54
Starting the Remote Access VPN Wizard 55
Configuring IPsec Remote Access Group Policy 55
Configuring WAN Settings 56
Configuring Operation Mode 56
Configuring Access Control Settings 57
Configuring DNS and WINS Settings 57
Configuring Backup Servers 58
Configuring Split Tunneling 58
Viewing Group Policy Summary 58
Configuring IPsec Remote Access User Groups 59
Viewing IPsec Remote Access Summary 59
Using Remote Access VPN Wizard for SSL Remote Access 60
Starting the Remote Access VPN Wizard with SSL Remote Access 60
Configuring SSL VPN Gateway 60
Configuring SSL VPN Group Policy 62
Configuring SSL VPN User Groups 65
Viewing SSL VPN Summary 66
Using the Site-to-Site VPN Wizard to Configure Site-to-Site VPN 66
Starting the Site-to-Site VPN Wizard 67
Configuring VPN Peer Settings 67
Configuring IKE Policies 68

Configuring Transform Policies 69
Configuring Local and Remote Networks 70
Viewing Configuration Summary 70
Using the DMZ Wizard to Configure DMZ Settings 71
Starting the DMZ Wizard 71
Configuring DDNS Profiles 71
Configuring DMZ Network 72
Configuring DMZ Services 74
Viewing Configuration Summary 76
Using the Wireless Wizard (for ISA550W and ISA570W only) 76
Starting the Wireless Wizard 76
Configuring Wireless Radio Settings 76
Configuring Wireless Connectivity Types 77
Specify Wireless Connectivity Settings for All Enabled SSIDs 78
Viewing Configuration Summary 78
Configuring the SSID for Intranet WLAN Access 78
Configuring the SSID for Guest WLAN Access 80

Chapter 3: Status 84

Device Status Dashboard 84
Network Status 88
Status Summary 88
Traffic Statistics 91
Usage Reports 92
WAN Bandwidth Reports 94
ARP Table 95
DHCP Bindings 95
STP Status 96
CDP Neighbor 98
Wireless Status (for ISA550W and ISA570W only) 99
Wireless Status 99
Client Status 100

NAT Status 100
VPN Status 101
IPsec VPN Status 101
SSL VPN Status 103
Active User Sessions 105
Security Services Reports 106
Web Security Report 106
Anti-Virus Report 107
Email Security Report 108
Network Reputation Report 109
IPS Report 110
Application Control Report 111
System Status 112
Processes 112
Resource Utilization 113

Chapter 4: Networking 115

Viewing Network Status 116
Configuring IPv4 or IPv6 Routing 116
Managing Ports 116
Viewing Status of Physical Interfaces 117
Configuring Physical Ports 118
Configuring Port Mirroring 119
Configuring Port-Based (802.1x) Access Control 120
Configuring the WAN 122
Configuring WAN Settings for Your Internet Connection 122
Configuring WAN Redundancy 130
Dual WAN Settings 130
Configuring Link Failover Detection 132
Load Balancing with Policy-Based Routing Configuration Example 133
Configuring Dynamic DNS 134
Measuring and Limiting Traffic with the Traffic Meter 135
Configuring a VLAN 137

Configuring DMZ 141
Configuring Zones 146
Security Levels for Zones 146
Predefined Zones 147
Configuring Zones 147
Configuring DHCP Reserved IPs 149
Configuring Routing 149
Viewing the Routing Table 150
Configuring Routing Mode 150
Configuring Static Routing 151
Configuring Dynamic Routing - RIP 152
Configuring Policy-Based Routing 153
Configuring Quality of Service 155
General QoS Settings 155
Configuring WAN QoS 156
Managing WAN Bandwidth for Upstream Traffic 156
Configuring WAN Queue Settings 157
Configuring Traffic Selectors 158
Configuring WAN QoS Policy Profiles 160
Configuring WAN QoS Class Rules 160
Mapping WAN QoS Policy Profiles to WAN Interfaces 161
WAN QoS Configuration Example 162
Configure WAN QoS for Voice Traffic from LAN to WAN 164
Configuring WAN QoS for Voice Traffic from WAN to LAN 165
Configuring LAN QoS 166
Configuring LAN Queue Settings 167
Configuring LAN QoS Classification Methods 167
Mapping CoS to LAN Queue 168
Mapping DSCP to LAN Queue 168
Configuring Default CoS 169
Configuring Wireless QoS 169
Default Wireless QoS Settings 169
Configuring Wireless QoS Classification Methods 170
Mapping CoS to Wireless Queue 171
Mapping DSCP to Wireless Queue 171
Understanding DSCP Values 171

Configuring IGMP 172
Configuring VRRP 173
Address Management 175
Configuring Addresses 175
Configuring Address Groups 176
Service Management 177
Configuring Services 177
Configuring Service Groups 178
Configuring Captive Portal 179
Requirements 179
Before You Begin 180
VLAN Setup 180
Wireless Setup 181
User Authentication 181
Configuring a Captive Portal 181
Troubleshooting 185
Using External Web-Hosted CGI Scripts 186
CGI Source Code Example: No Authentication and Accept Button 195
Related Information 204

Chapter 5: Wireless (for ISA550W and ISA570W only) 206

Viewing Wireless Status 207
Viewing Wireless Statistics 207
Viewing Wireless Client Status 208
Configuring the Basic Settings 208
Configuring SSID Profiles 210
Configuring Wireless Security 211
Controlling Wireless Access Based on MAC Addresses 217
Mapping the SSID to VLAN 218
Configuring SSID Schedule 218
Configuring Wi-Fi Protected Setup 219
Configuring Captive Portal 221

Requirements 222
Before You Begin 222
VLAN Setup 222
Wireless Setup 223
User Authentication 223
Configuring a Captive Portal 223
Troubleshooting 227
Using External Web-Hosted CGI Scripts 228
CGI Source Code Example: No Authentication and Accept Button 237
Related Information 246
Configuring Wireless Rogue AP Detection 247
Advanced Radio Settings 248

Chapter 6: Firewall 251

Configuring Firewall Rules to Control Inbound and Outbound Traffic 252
About Security Zones 252
Default Firewall Settings 254
Priorities of Firewall Rules 255
Preliminary Tasks for Configuring Firewall Rules 255
General Firewall Settings 256
Configuring a Firewall Rule 257
Configuring a Firewall Rule to Allow Multicast Traffic 259
Configuring Firewall Logging Settings 260
Configuring NAT Rules to Securely Access a Remote Network 261
Viewing NAT Translation Status 262
Priorities of NAT Rules 263
Configuring Dynamic PAT Rules 264
Configuring Static NAT Rules 265
Configuring Port Forwarding Rules 266
Configuring Port Triggering Rules 268
Configuring Advanced NAT Rules 269
Configuring IP Alias for Advanced NAT rules 270

Configuring an Advanced NAT Rule to Support NAT Hairpinning 272
Firewall and NAT Rule Configuration Examples 274
Allowing Inbound Traffic Using the WAN IP Address 274
Allowing Inbound Traffic Using a Public IP Address 276
Allowing Inbound Traffic from Specified Range of Outside Hosts 279
Blocking Outbound Traffic by Schedule and IP Address Range 280
Blocking Outbound Traffic to an Offsite Mail Server 280
Configuring Content Filtering to Control Internet Access 281
Configuring Content Filtering Policy Profiles 281
Configuring Website Access Control List 282
Mapping Content Filtering Policy Profiles to Zones 283
Configuring Advanced Content Filtering Settings 284
Configuring MAC Address Filtering to Permit or Block Traffic 285
Configuring IP-MAC Binding to Prevent Spoofing 286
Configuring Attack Protection 287
Configuring Session Limits 288
Configuring Application Level Gateway 289

Chapter 7: Security Services 291

About Security Services 292
Activating Security Services 293
Priority of Security Services 293
Security Services Dashboard 294
Viewing Security Services Reports 295
Viewing Web Security Report 296
Viewing Anti-Virus Report 297
Viewing Email Security Report 298
Viewing Network Reputation Report 299
Viewing IPS Report 300
Viewing Application Control Report 301
Configuring Anti-Virus 302
General Anti-Virus Settings 303

Configuring Advanced Anti-Virus Settings 306
Configuring HTTP Notification 307
Configuring Email Notification 307
Updating Anti-Virus Signatures 308
Configuring Application Control 309
Configuring Application Control Policies 310
General Application Control Policy Settings 310
Adding an Application Control Policy 311
Permitting or Blocking Traffic for all Applications in a Category 312
Permitting or Blocking Traffic for an Application 313
General Application Control Settings 314
Enabling Application Control Service 315
Mapping Application Control Policies to Zones 315
Configuring Application Control Policy Mapping Rules 316
Updating Application Signature Database 317
Advanced Application Control Settings 318
Configuring Spam Filter 319
Configuring Intrusion Prevention 321
Configuring Signature Actions 323
Updating IPS Signature Database 324
Configuring Web Reputation Filtering 325
Configuring Web URL Filtering 327
Configuring Web URL Filtering Policy Profiles 328
Configuring Website Access Control List 329
Mapping Web URL Filtering Policy Profiles to Zones 330
Configuring Advanced Web URL Filtering Settings 330
Network Reputation 332

Chapter 8: VPN 333

About VPNs 334
Viewing VPN Status 335
Viewing IPsec VPN Status 335
Viewing SSL VPN Status 337
Configuring a Site-to-Site VPN 340

Configuration Tasks to Establish a Site-to-Site VPN Tunnel 341
General Site-to-Site VPN Settings 341
Configuring IPsec VPN Policies 343
Configuring IKE Policies 349
Configuring Transform Sets 351
Remote Teleworker Configuration Examples 352
Configuring IPsec Remote Access 355
Cisco VPN Client Compatibility 356
Enabling IPsec Remote Access 357
Configuring IPsec Remote Access Group Policies 357
Allowing IPsec Remote VPN Clients to Access the Internet 360
Configuring Teleworker VPN Client 363
Required IPsec VPN Servers 364
Benefits of the Teleworker VPN Client Feature 365
Modes of Operation 365
Client Mode 366
Network Extension Mode 367
General Teleworker VPN Client Settings 368
Configuring Teleworker VPN Client Group Policies 369
Configuring SSL VPN 372
Elements of the SSL VPN 373
Configuration Tasks to Establish a SSL VPN Tunnel 374
Installing Cisco AnyConnect Secure Mobility Client 375
Importing Certificates for User Authentication 376
Configuring SSL VPN Users 376
Configuring SSL VPN Gateway 376
Configuring SSL VPN Group Policies 379
Accessing SSL VPN Portal 382
Allowing SSL VPN Clients to Access the Internet 382
Configuring L2TP Server 385
Configuring VPN Passthrough 387

Chapter 9: User Management 388

Viewing Active User Sessions 388
Configuring Users and User Groups 389
Default User and User Group 389
Available Services for User Groups 389
Preempt Administrators 390
Configuring Local Users 390
Configuring Local User Groups 391
Configuring User Authentication Settings 393
Using Local Database for User Authentication 394
Using RADIUS Server for User Authentication 394
Using Local Database and RADIUS Server for User Authentication 397
Using LDAP for User Authentication 398
Using Local Database and LDAP for Authentication 400
Configuring RADIUS Servers 401

Chapter 10: Device Management 403

Viewing System Status 404
Viewing Process Status 404
Viewing Resource Utilization 404
Administration 405
Configuring Administrator Settings 406
Configuring Remote Administration 407
Configuring Email Alert Settings 408
Configuring SNMP 415
Backing Up and Restoring a Configuration 416
Managing Certificates for Authentication 418
Viewing Certificate Status and Details 419
Exporting Certificates to Your Local PC 420
Exporting Certificates to a USB Device 421
Importing Certificates from Your Local PC 421
Importing Certificates from a USB Device 422

Generating New Certificate Signing Requests 422
Importing Signed Certificate for CSR from Your Local PC 423
Configuring Cisco Services and Support Settings 424
Configuring Cisco.com Account 424
Configuring Cisco OnPlus 425
Configuring Remote Support Settings 426
Sending Contents for System Diagnosis 426
Configuring System Time 427
Configuring Device Properties 428
Diagnostic Utilities 428
Ping 429
Traceroute 429
DNS Lookup 430
Packet Capture 430
Device Discovery Protocols 430
UPnP Discovery 431
Bonjour Discovery 432
CDP Discovery 432
LLDP Discovery 433
Firmware Management 434
Viewing Firmware Information 435
Using the Secondary Firmware 435
Upgrading your Firmware from Cisco.com 436
Upgrading Firmware from a PC or a USB Device 437
Firmware Auto Fall Back Mechanism 438
Using Rescue Mode to Recover the System 438
Managing Security License 439
Checking Security License Status 440
Installing or Renewing Security License 441
Log Management 442
Viewing Logs 442
Configuring Log Settings 444

Configuring Log Facilities 447
Rebooting and Resetting the Device 448
Restoring the Factory Default Settings 448
Rebooting the Security Appliance 449
Configuring Schedules 449

Appendix A: Troubleshooting 453

Internet Connection 453
Date and Time 456
Pinging to Test LAN Connectivity 457
Testing the LAN Path from Your PC to Your Security Appliance 457
Testing the LAN Path from Your PC to a Remote Device 458

Appendix B: Technical Specifications and Environmental Requirements 459

Appendix C: Factory Default Settings 461

Device Management 461
User Management 463
Networking 464
Wireless 468
VPN 469
Security Services 471
Firewall 471
Reports 473
Default Service Objects 474
Default Address Objects 478

Appendix D: Where to Go From Here 479

1

Getting Started

This chapter provides an overview of the Cisco ISA500 Series Integrated Security Appliance and describes basic configuration tasks to help you configure your security appliance. It includes the following sections:

- **Introduction, page 20**
- **Product Overview, page 21**
- **Getting Started with the Configuration Utility, page 25**
- **Factory Default Settings, page 30**
- **Performing Basic Configuration Tasks, page 32**

NOTE For information about how to physically install your security appliance, see the Cisco ISA500 Series Integrated Security Appliances Quick Start Guide at: www.cisco.com/go/isa500resources.

Introduction

Thank you for choosing the Cisco ISA500 Series Integrated Security Appliance, a member of the Small Business Family. The ISA500 Series is a set of Unified Threat Management (UTM) security appliances that provide business-class security gateway solutions with dual WAN, DMZ, zone-based firewall, site-to-site and remote access VPN (including IPsec Remote Access, Teleworker VPN Client, and SSL VPN) support, and Internet threat protection, such as Intrusion Prevention (IPS), Anti-Virus, Application Control, Web URL Filtering, Web Reputation Filtering, Spam Filter, and Network Reputation. The ISA550W and ISA570W include 802.11b/g/n access point capabilities.

The following table lists the available model numbers.

Model	Description	Configuration
ISA550	Cisco ISA550 Integrated Security Appliance	1 WAN port, 2 LAN ports, 4 configurable ports, and 1 USB 2.0 port
ISA550W	Cisco ISA550 Integrated Security Appliance with Wi-Fi	1 WAN port, 2 LAN ports, 4 configurable ports, 1 USB 2.0 port, and 802.11b/g/n
ISA570	Cisco ISA570 Integrated Security Appliance	1 WAN port, 4 LAN ports, 5 configurable ports, and 1 USB 2.0 port
ISA570W	Cisco ISA570 Integrated Security Appliance with Wi-Fi	1 WAN port, 4 LAN ports, 5 configurable ports, 1 USB 2.0 port, and 802.11b/g/n

NOTE Any configurable port can be configured to be a WAN, DMZ, or LAN port. Only one configurable port can be configured as a WAN port at a time. Up to 4 configurable ports can be configured as DMZ ports.

Product Overview

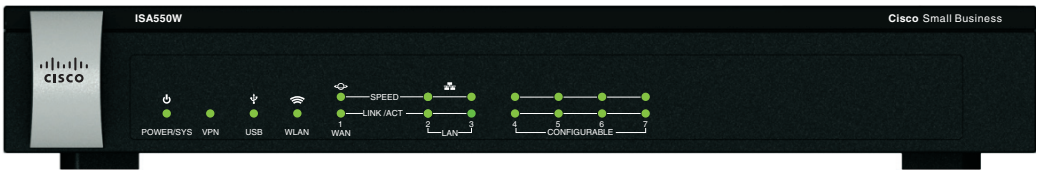
Before you use the security appliance, become familiar with the lights on the front panel and the ports on the rear panel.

- Front Panel, page 21
- Back Panel, page 23

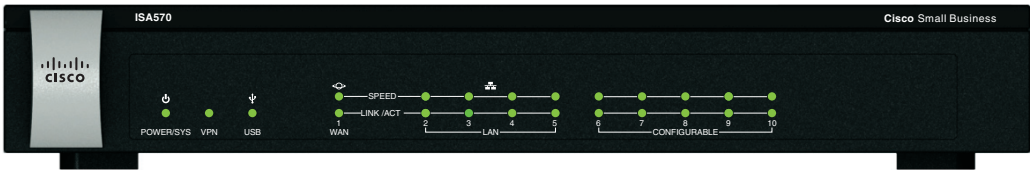
Front Panel

ISA550 Front Panel

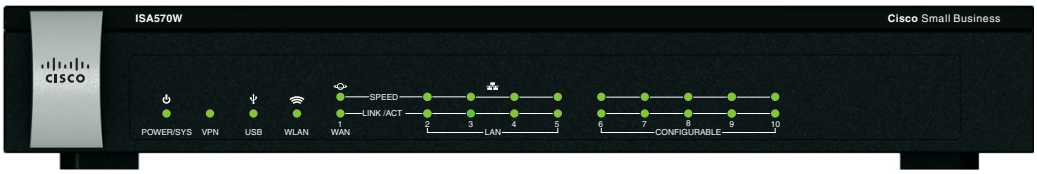
ISA550W Front Panel



ISA570 Front Panel



ISA570W Front Panel



Front Panel Lights

The following table describes the lights on the front panel of the security appliance. These lights are used for monitoring system activity.

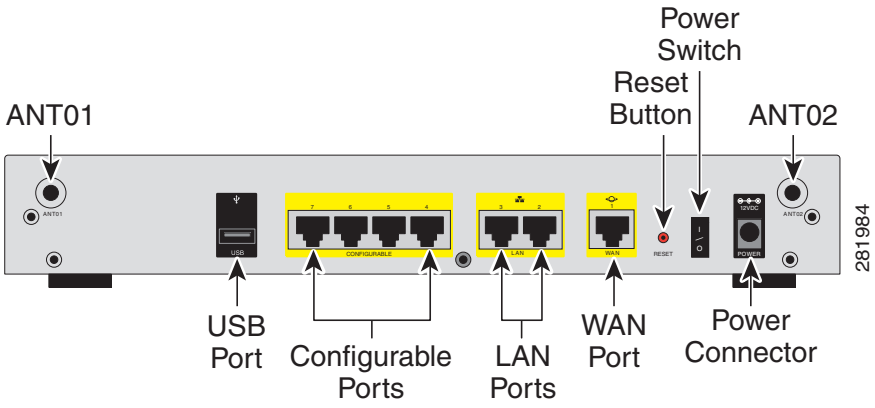
Light	Description
POWER/SYS	Indicates the power and system status. ▪ Solid green when the system is powered on and is operating normally. ▪ Flashes green when the system is booting. ▪ Solid amber when the system has a booting problem, a device error occurs, or the system has a problem.
VPN	Indicates the site-to-site VPN connection status. ▪ Solid green when there are active site-to-site VPN connections. ▪ Flashes green when attempting to establish a site-to-site VPN tunnel. ▪ Flashes amber when the system is experiencing problems setting up a site-to-site VPN connection and there is no VPN connection.
USB	Indicates the USB device status. ▪ Solid green when a USB device is detected and is operating normally. ▪ Flashes green when the USB device is transmitting and receiving data.
WLAN **(ISA550W and ISA570W only)**	Indicates the WLAN status. ▪ Solid green when the WLAN is up. ▪ Flashes green when the WLAN is transmitting and receiving data.

Light	Description
SPEED	Indicates the traffic rate of the associated port. ▪ Off when the traffic rate is 10 or 100 Mbps. ▪ Solid green when the traffic rate is 1000 Mbps.
LINK/ACT	Indicates that a connection is being made through the port. ▪ Solid green when the link is up. ▪ Flashes green when the port is transmitting and receiving data.

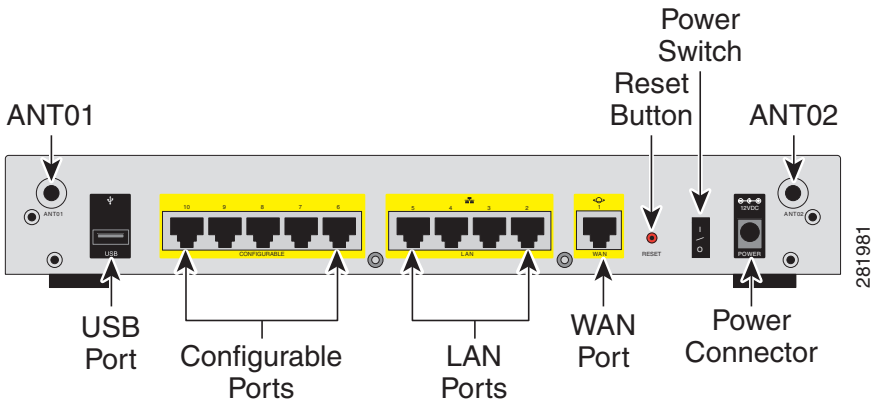
Back Panel

The back panel is where you connect the network devices. The ports on the panel vary depending on the model.

ISA550 and ISA550W Back Panel



ISA570 and ISA570W Back Panel



Back Panel Descriptions

Feature	Description
ANT01/ANT02	Threaded connectors for the antennas **(for ISA550W and ISA570W only)**.
USB Port	Connects the unit to a USB device. You can use a USB device to save and restore system configuration, or to upgrade the firmware.
Configurable Ports	Can be set to operate as WAN, LAN, or DMZ ports. ISA550 and ISA550W have 4 configurable ports. ISA570 and ISA570W have 5 configurable ports. **NOTE:** Only one configurable port can be configured as a WAN port at a time. Up to 4 configurable ports can be configured as DMZ ports.
LAN Ports	Connects PCs and other network appliances to the unit. ISA550 and ISA550W have 2 dedicated LAN ports. ISA570 and ISA570W have 4 dedicated LAN ports.
WAN Port	Connects the unit to a DSL or a cable modem, or other WAN connectivity device.

Feature	Description
RESET Button	To reboot the unit, push and release the RESET button for less than 3 seconds. To restore the unit to its factory default settings, push and hold the RESET button for more than 3 seconds while the unit is powered on and the POWER/SYS light is solid green. The POWER/SYS light will flash green when the system is rebooting.
Power Switch	Powers the unit on or off.
Power Connector	Connects the unit to power using the supplied power cord and adapter.

Getting Started with the Configuration Utility

The ISA500 Series Configuration Utility is a web-based device manager that is used to provision the security appliance. To use this utility, you must be able to connect to the security appliance from a PC or laptop. You can access the Configuration Utility by using the following web browsers:

- Microsoft Internet Explorer 8 and 9
- Mozilla Firefox 3.6.x, 5, and 6

NOTE The minimum recommended display resolution for the PC running the Web browser used to access the Configuration Utility is 1024 x 768.

This section includes the following topics:

- **Logging in to the Configuration Utility, page 26**
- **Navigating Through the Configuration Utility, page 27**
- **Using the Help System, page 28**
- **Configuration Utility Icons, page 28**

Logging in to the Configuration Utility

STEP 1 Connect your computer to an available LAN port on the back panel.

Your PC will become a DHCP client of the security appliance and will receive an IP address in the 192.168.75.x range.

STEP 2 Start a web browser. In the address bar, enter the default IP address of the security appliance: **192.168.75.1**.

NOTE: The above address is the factory default LAN address. If you change this setting, enter the new IP address to connect to the Configuration Utility.

STEP 3 When the login page opens, enter the username and password.

The default username is **cisco**. The default password is **cisco**. Usernames and passwords are case sensitive.

STEP 4 Click **Login**.

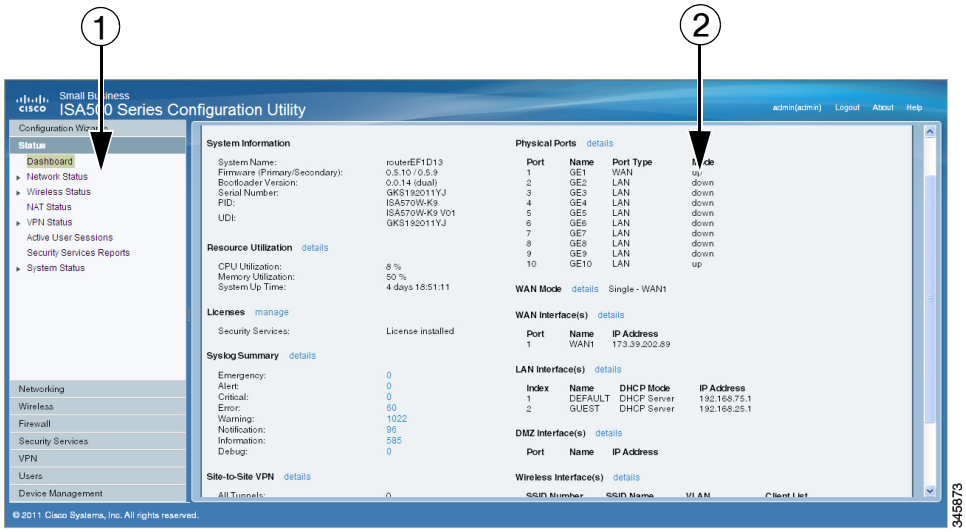
STEP 5 For security purposes, you must change the default password of the default administrator account. Set a new administrator password and click **OK**.

STEP 6 If you can access the Internet and a newer firmware is detected, the Firmware Upgrade window opens. Follow the on-screen prompts to download and install the firmware. See **Upgrading your Firmware After your First Login, page 33**.

STEP 7 If you cannot access the Internet or you are using the latest firmware, the Setup Wizard will now launch. Follow the on-screen prompts to complete the initial configuration. See Using the Setup Wizard for the Initial Configuration, page 36.

Navigating Through the Configuration Utility

Use the left hand navigation pane to perform the tasks in the Configuration Utility.



Number	Component	Description
1	Left Hand Navigation Pane	The left hand navigation pane provides easy navigation through the configurable features. The main branches expand to provide the features. Click the main branch title to expand its contents. Click the triangle next to a feature to expand or contract its sub-features. Click the title of a feature or sub-feature to open it.
2	Main Content	The main content of the feature or sub-feature appears in this area.

Using the Help System

The Configuration Utility provides a context-sensitive help file for all configuration tasks. To view the Help page, click the **Help** link in the top right corner of the screen. A new window opens with information about the page that you are currently viewing.

Configuration Utility Icons

The Configuration Utility has icons for commonly used configuration options. The following table describes these icons:

Icon	Description	Action
	Add icon	Add an entry.
	Edit icon	Edit an entry.
	Duplicate icon	Create a copy of an existing entry.
	Delete icon	Delete an entry or delete multiple selected entries.
	Move icon	Move an item to a specific location.
	Move down icon	Move an item down one position.
	Move up icon	Move an item up one position.
	Expand triangle icon	Expand the sub-features of a feature in the left navigation pane or expand the items under a category.
	Contract triangle icon	Contract the sub-features of a feature in the left navigation pane or contract the items under a category.
	Connect icon	Establish a VPN connection.
	Disconnect or Logout icon	Terminate a VPN connection or an active user session.

Icon	Description	Action
	Forced Authorized icon	Disable 802.1x access control and cause the port to transition to the authorized state without any authentication exchange required.
	Forced Unauthorized icon	Cause the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate.
	Auto icon	Enable 802.1x access control and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port.
	Import PC icon	Import a local certificate or a CA certificate from PC.
	Export to USB or Import from USB icon	Export a local certificate, a CA certificate, or a Certificate Signing Request to a USB key, or import a local certificate or a CA certificate from a USB key.
	Details icon	View the details of a certificate or a Certificate Signing Request.
	Download icon	Download a local certificate, a CA certificate, or a Certificate Signing Request to PC.
	Upload icon	Upload a signed certificate for the Certificate Signing Request from PC.
	Install or Renew icon	Install the security license.
	Refresh icon	Refresh the data.
	Reset icon	Reset the device to the factory defaults, or renew the security license.
	Check for Updates Now icon	Check for new signature updates from Cisco's signature server immediately.
	Credentials icon	View the device credentials.
	Email Alerts icon	View or configure the email alert settings.

Factory Default Settings

The security appliance is preconfigured with settings to allow you to start using the device with minimal changes. Depending on the requirements of your Internet Service Provider (ISP) and the needs of your business, you may need to modify some of these settings. You can use the Configuration Utility to customize all settings, as needed.

This section includes the following topics:

- **Default Settings of Key Features, page 30**
- **Restoring the Factory Default Settings, page 31**

Default Settings of Key Features

The default settings of key features are described below. For a full list of all factory default settings, see Factory Default Settings, page 461.

- **IP Routing Mode:** By default, only the IPv4 mode is enabled. To support IPv4 and IPv6 addressing, enable the IPv4/IPv6 mode. See Configuring IPv4 or IPv6 Routing, page 116.
- **WAN Configuration:** By default, the security appliance is configured to obtain an IP address from your ISP using Dynamic Host Configuration Protocol (DHCP). Depending on the requirement of your ISP, configure the network addressing mode for the primary WAN. You can change other WAN settings as well. See Configuring WAN Settings for Your Internet Connection, page 122.
- **LAN Configuration:** By default, the LAN of the security appliance is configured in the 192.168.75.0 subnet and the LAN IP address is 192.168.75.1. The security appliance acts as a DHCP server to the hosts on the LAN network. It can automatically assign IP addresses and DNS server addresses to the PCs and other devices on the LAN. For most deployment scenarios, the default DHCP and TCP/IP settings should be satisfactory. However, you can change the subnet address or the default IP address. See Configuring a VLAN, page 137.
- **VLAN Configuration:** The security appliance predefines a native VLAN (DEFAULT) and a guest VLAN (GUEST). You can customize the predefined VLANs or create new VLANs for your specific business needs. See Configuring a VLAN, page 137.

- **Configurable Ports:** Any configurable port can be configured to be a WAN, DMZ, or LAN port. By default, all configurable ports are set to be LAN ports. Only one configurable port can be configured as a WAN port at a time (See Configuring the WAN, page 122). Up to four configurable ports can be configured as DMZ ports (see Configuring DMZ, page 141).
- **Wireless Network (for ISA550W and ISA570W only):** ISA550W and ISA570W are configured with four SSIDs. All SSIDs are disabled by default. For security purposes, we strongly recommend that you configure the SSIDs with the appropriate security settings. See Wireless (for ISA550W and ISA570W only), page 206.
- **Administrative Access:** You can access the Configuration Utility by using a web browser from the LAN side and entering the default LAN IP address of 192.168.75.1. You can log on by entering the username (**cisco**) and password (**cisco**) of the default administrator account. To prevent unauthorized access, you must immediately change the administrator password at the first login and are encouraged to change the username for the default administrator account. See Changing the Default Administrator Password, page 32.
- **Security Services:** By default, the security services such as Intrusion Prevention (IPS), Anti-Virus, Application Control, Web URL Filtering, Web Reputation Filtering, and Spam Filter are disabled. See **Chapter 7, "Security Services."**
- **Firewall:** By default, the firewall prevents inbound traffic and allows all outbound traffic. If you want to allow some inbound traffic or prevent some outbound traffic, you must customize firewall rules. Up to 100 custom firewall rules can be configured on the security appliance. See Configuring Firewall Rules to Control Inbound and Outbound Traffic, page 252.
- **VPN:** By default, the VPN feature is disabled. The security appliance can function as an IPsec VPN server, a Teleworker VPN client, or as a SSL VPN gateway so that remote users can securely access the corporate network resources over the VPN tunnels. You can also establish a secure IPsec VPN tunnel between two sites that are physically separated by using the Site-to-Site VPN feature. See VPN, page 333.

Restoring the Factory Default Settings

To restore the factory defaults, choose one of the following actions:

- Press and hold the **RESET** button on the back panel of the unit for more than 3 seconds while the unit is powered on and the POWER/SYS light is solid

green. Release the button and wait for the unit to reboot. The POWER/SYS light will flash green when the system is rebooting.

- Or launch the Configuration Utility and login. Click **Device Management > Reboot/Reset** in the left hand navigation pane. In the **Reset Device** area, click **Reset to Factory Defaults**.

After a restore to factory defaults, the following settings apply:

Parameter	Default Value
Username	cisco
Password	cisco
LAN IP	192.168.75.1
DHCP Range	192.168.75.100 to 200

Performing Basic Configuration Tasks

We recommend that you complete the following tasks before you configure the security appliance:

- **Changing the Default Administrator Password, page 32**
- **Upgrading your Firmware After your First Login, page 33**
- **Backing Up Your Configuration, page 34**

Changing the Default Administrator Password

The default administrator account (“cisco”) has full privilege to set the configuration and read the system status. For security purposes, you must change the default administrator password at the first login.

STEP 1 Enter the following information:

- **User name:** Enter the current username or enter a new username if you want to change the default username.

- **New password:** Enter a new administrator password. Passwords are case sensitive.

  NOTE: A password requires a minimum of 8 characters, including at least three of these character classes: uppercase letters, lowercase letters, digits, and special characters. Do not repeat any password more than three times in a row. Do not set the password as the username or "cisco." Do not capitalize or spell these words backwards.

- **Confirm password:** Enter the new administrator password again for confirmation.

STEP 2 Click **OK** to save your settings.

Upgrading your Firmware After your First Login

The security appliance uses a built-in IDA client to query the firmware from Cisco's IDA server. If a newer firmware is detected after you log in to the Configuration Utility for the first time, we recommend that you upgrade your firmware to the latest version before you do any other tasks. This feature requires that you have an active WAN connection to access the Internet.

STEP 1 Log in to the Configuration Utility for the first time and change the default administrator password. See **Logging in to the Configuration Utility, page 26**.

If newer firmware is detected, the Firmware Upgrade window opens. The version number for the firmware that you are currently using and the version number for the latest firmware that is detected are displayed.

STEP 2 Enter your Cisco.com account credentials in the **Username** and **Password** fields.

A valid Cisco.com account is required to download and install the firmware from Cisco.com. If you do not have one, go to this page:
https:// tools.cisco.com/RPF/register/register.do
Then click the **Create a Cisco.com Account** link to register a Cisco.com account.

NOTE: Skip this step if your Cisco.com account credentials are already configured on the security appliance.

STEP 3 Click **Continue**.

NOTE: You can click **Install Later** to upgrade the firmware later. An **Upgrade Available** link will be displayed at the top right corner of the screen and the Setup Wizard will now launch. We strongly recommend that you upgrade the firmware immediately.

STEP 4 Validate your Cisco.com account credentials through the Internet. If your Cisco.com account credentials are valid, the security appliance starts downloading and installing the firmware. This process will take several minutes.

STEP 5 The security appliance reboots after the firmware is upgraded. You will be redirected to the login screen when the security appliance boots up.

STEP 6 Log in to the Configuration Utility again. The Setup Wizard will launch. Follow the on-screen prompts to complete the initial configuration. See Using the Setup Wizard for the Initial Configuration, page 36.

NOTE Other options to upgrade the firmware:

- If you cannot access the Internet after you log in to the Configuration Utility for the first time, you can use the Setup Wizard to configure your Internet connection and then automatically check for firmware updates after the Setup Wizard is complete. The Setup Wizard also allows you to manually upgrade the firmware from a firmware image stored on your local PC. See Using the Setup Wizard for the Initial Configuration, page 36.
- You can manually upgrade the firmware from a firmware image stored on your PC or on a USB device. You must first download the latest firmware image from Cisco.com and save it to your local PC or to a USB device. See Upgrading Firmware from a PC or a USB Device, page 437.
- The security appliance automatically checks for firmware updates from Cisco's IDA server every 24 hours. You can upgrade your firmware to the latest version if a newer firmware is available on Cisco.com. This feature requires that you have an active WAN connection and a valid Cisco.com account is configured on the security appliance in advance. See Upgrading your Firmware from Cisco.com, page 436.

Backing Up Your Configuration

At any point during the configuration process, you can back up your configuration. Later, if you make changes that you want to abandon, you can easily restore the saved configuration. See Backing Up and Restoring a Configuration, page 416.

2

Configuration Wizards

This chapter describes how to use the configuration wizards to configure the security appliance. It includes the following sections:

- **Using the Setup Wizard for the Initial Configuration, page 36**
- **Using the Dual WAN Wizard to Configure WAN Redundancy Settings, page 51**
- **Using the Remote Access VPN Wizard, page 54**
- **Using the Site-to-Site VPN Wizard to Configure Site-to-Site VPN, page 66**
- **Using the DMZ Wizard to Configure DMZ Settings, page 71**
- **Using the Wireless Wizard (for ISA550W and ISA570W only), page 76**

To access the Configuration Wizards pages, click **Configuration Wizards** in the left hand navigation pane.

Using the Setup Wizard for the Initial Configuration

Use the Setup Wizard to quickly configure the primary features of your security appliance, such as Cisco.com account credentials, security license, remote administration, port, WAN, LAN, DMZ, WAN redundancy, WLAN (for ISA550W and ISA570W only), and security services. Refer to the following steps:

- Starting the Setup Wizard, page 37
- Configuring Cisco.com Account Credentials, page 37
- Enabling Firmware Upgrade, page 38
- Validating Security License, page 39
- Enabling Bonjour and CDP Discovery Protocols, page 39
- Configuring Remote Administration, page 40
- Configuring Physical Ports, page 41
- Configuring the Primary WAN, page 42
- Configuring the Secondary WAN, page 42
- Configuring WAN Redundancy, page 42
- Configuring Default LAN Settings, page 43
- Configuring DMZ, page 44
- Configuring DMZ Services, page 45
- Configuring Wireless Radio Settings, page 47
- Configuring Intranet WLAN Access, page 48
- Configure Security Services, page 49
- Viewing Configuration Summary, page 50

NOTE Before you use the Setup Wizard to configure your security appliance, we recommend that you have the following requirements:

- An active WAN connection for verifying your Cisco.com account credentials, validating the security license, and upgrading your firmware to the latest version from Cisco.com.

- A valid Cisco.com account for validating the security license and upgrading your firmware to the latest version from Cisco.com. To register a Cisco.com account, go to https:// tools.cisco.com/RPF/register/register.do.
- The Product Authorization Key (PAK), or license code, for validating the security license and activating security services. You can find the license code from the Software License Claim Certificate that Cisco provides upon purchase of the security appliance.

Starting the Setup Wizard

STEP 1 When you log in to the Configuration Utility for the first time, the Setup Wizard may launch automatically. To launch the Setup Wizard at any time, click **Configuration Wizards > Setup Wizard**.

The Getting Started page appears If you have applied a configuration, a warning message appears saying “Continuing with the Setup Wizard will overwrite some of your previously modified parameters.” Read the warning message carefully before you start configuring.

STEP 2 Click **Next**.

Configuring Cisco.com Account Credentials

STEP 3 Use the Cisco.com Credentials page to configure your Cisco.com account credentials.

A valid Cisco.com account is required to download the latest firmware image from Cisco.com, validate the security license, and check for signature updates from Cisco’s signature server for IPS, Application Control, and Anti-Virus. If you do not already have one, go to https:// tools.cisco.com/RPF/register/register.do by clicking the **Create a Cisco.com Account** link to register a Cisco.com account.

- **Username:** Enter the username of your Cisco.com account.
- **Password:** Enter the password of your Cisco.com account.

STEP 4 Click **Next**.

If you can access the Internet, the Setup Wizard will validate your Cisco.com account credentials through the Internet after you click **Next**.

If you cannot access the Internet, the Setup Wizard will assume that your Cisco.com account credentials are valid and proceed to next step.

NOTE: You can configure your Cisco.com account credentials on the Device Management > Cisco Services & Support > Cisco.com Account page after the Setup Wizard is complete. See Configuring Cisco.com Account, page 424.

STEP 5 If your Cisco.com account credentials are invalid, click **OK** to return to the Cisco.com Credentials page. Correct your Cisco.com account credentials and then click **Next** to verify them again.

STEP 6 If your Cisco.com account credentials are valid, proceed to the Upgrade Firmware page.

Enabling Firmware Upgrade

STEP 7 Use the Upgrade Firmware page to enable the device to check for firmware updates or to manually upgrade the firmware.

- To automatically check for firmware updates, check the box next to **Check for firmware update when Setup Wizard completes**. The security appliance will immediately check for firmware updates after the Setup Wizard is complete. This feature requires that you have an active WAN connection.
- To manually upgrade the firmware from a firmware image stored on your PC, uncheck the box next to **Check for firmware update when Setup Wizard completes**. Uncheck this box when you do not have an active WAN connection and you have already downloaded the latest firmware image from Cisco.com to your local PC.

STEP 8 If you uncheck the box, click **Browse** to locate and select the firmware image from your PC, and then click **Upgrade**.

After you click Upgrade, the security appliance starts installing the firmware. This process will take several minutes. Do not disconnect the power or reset the device. Doing so will cancel the firmware upgrade process and could possibly corrupt. The security appliance reboots after the firmware is upgraded. You will be redirected to the login screen when the security appliance boots up.

STEP 9 If you choose to automatically check for firmware updates, click **Next**.

Validating Security License

STEP 10 Use the License Installation page to validate the security license, which is used to activate security services on the device.

STEP 11 If the security license is already installed on the security appliance, click **Next** to proceed next step.

STEP 12 If the security license is not installed on the security appliance, enter the following information to validate the security license:

- **Email Address:** Enter the registered email address to receive the PAK ID.
- **PAK ID:** Enter your Product Authorization Key in this field. You can find the license code from the Software License Claim Certificate that Cisco provides upon purchase of the security appliance.

  NOTE: A valid Cisco.com account is required to validate the security license. If your Cisco.com account credentials are not configured, go back to the Cisco.com Credentials page to configure them.

NOTE: If you want to continue the Setup Wizard configuration without installing the security license, check the box next to **Continue without installing license (not recommended)**. The security services cannot be activated without installing the security license.

STEP 13 After you are finished, click **Next**.

Enabling Bonjour and CDP Discovery Protocols

STEP 14 Use the Discovery page to enable Bonjour and/or CDP discovery protocols on the security appliance. For optimal device discovery and topology support via the OnPlus portal, enable both discovery protocols.

- **Enable Bonjour Discovery Protocol:** Check this box to enable Bonjour discovery protocol, or uncheck this box to disable it.
- **Enable Cisco Discovery Protocol (CDP):** Check this box to enable Cisco Discovery Protocol (CDP), or uncheck this box to disable it.

  NOTE: Discovery protocols are only operational on the LAN ports of the security appliance.

STEP 15 After you are finished, click **Next**.

Configuring Remote Administration

STEP 16 Use the Remote Administration page to configure the remote management settings. The security appliance allows remote management securely by using HTTPS and HTTP, for example https://xxx.xxx.xxx.xxx:8080.

- **Remote Administration:** Click **On** to enable remote management by using HTTPS, or click **Off** to disable it. We recommend that you use HTTPS for secure remote management.
- **HTTPS Listen Port Number:** If you enable remote management by using HTTPS, enter the port number. By default, the listen port number for HTTPS is 8080.
- **HTTP Enable:** Click **On** to enable remote management by using HTTP, or click **Off** to disable it.
- **HTTP Listen Port Number:** If you enable remote management by using HTTP, enter the port number. By default, the listen port number for HTTP is 80.
- **Allow Address:** To specify the devices that can access the configuration utility through the WAN interface, choose an Address Object or enter an address.
  - **Address Objects:** These objects represent known IP addresses and address ranges, such as the GUEST VLAN and the DHCP pool. After completing the wizard, you can view information about Address Objects on the Networking > Address Management page.
  - **Create new address:** Choose this option to enter an IP address or address range. In the pop-up window, enter a **Name** and specify the **Type** (Host or Range). For a single host, enter the IP address. For a range, enter the **Starting IP Address** and the **Ending IP Address**.
- **Remote SNMP:** Click **On** to enable SNMP for remote connection, or click **Off** to disable SNMP. Enabling SNMP allows remote users to use the SNMP protocol to access the Configuration Utility.

STEP 17 After you are finished, click **Next**.

Configuring Physical Ports

STEP 18 Use the Port Configuration page to specify the port configuration.

If you are using the ISA570 or ISA570W, choose one of the following options:

- **1 WAN, 9 LAN switch:** One WAN port (WAN1) and nine LAN ports are configured.
- **1 WAN, 1 DMZ, 8 LAN switch:** One WAN port (WAN1), one DMZ port, and eight LAN ports are configured. The configurable port GE10 is set as a DMZ port.
- **1 WAN, 1 WAN backup, 8 LAN switch:** Two WAN ports (WAN1 is the primary WAN and WAN2 is the secondary WAN) and eight LAN ports are configured. The configurable port GE10 is set as the secondary WAN port.
- **1 WAN, 1 WAN backup, 1 DMZ, 7 LAN switch:** Two WAN ports (WAN1 is the primary WAN and WAN2 is the secondary WAN), one DMZ port, and seven LAN ports are configured. The configurable port GE10 is set as the secondary WAN port and the configurable port GE9 is set as a DMZ port.

If you are using the ISA550 or ISA550W, choose one of the following options:

- **1 WAN, 6 LAN switch:** One WAN port (WAN1) and six LAN ports are configured.
- **1 WAN, 1 DMZ, 5 LAN switch:** One WAN port (WAN1), one DMZ port, and five LAN ports are configured. The configurable port GE7 is set as a DMZ port.
- **1 WAN, 1 WAN backup, 5 LAN switch:** Two WAN ports (WAN1 is the primary WAN and WAN2 is the secondary WAN) and five LAN ports are configured. The configurable port GE7 is set as the secondary WAN port.
- **1 WAN, 1 WAN backup, 1 DMZ, 4 LAN switch:** Two WAN ports (WAN1 is the primary WAN and WAN2 is the secondary WAN), one DMZ port, and four LAN ports are configured. The configurable port GE7 is set as the secondary WAN port and the configurable port GE6 is set as a DMZ port.

NOTE: If you have two ISP links, we recommend that you set a backup WAN so that you can provide backup connectivity or load balancing. If you need to host public services, we recommend that you set a DMZ port.

STEP 19 After you are finished, click **Next**.

Configuring the Primary WAN

STEP 20 Use the Primary WAN Connection page to configure the primary WAN connection by using the account information provided by your ISP.

- **WAN Name:** The name of the primary WAN port.
- **IP Address Assignment:** Depending on the requirements of your ISP, choose the network addressing mode and configure the corresponding fields for the primary WAN port. The security appliance supports DHCP Client, Static IP, PPPoE, PPTP, and L2TP. For complete details, see Network Addressing Mode, page 125.

STEP 21 After you are finished, click **Next**.

Configuring the Secondary WAN

STEP 22 If only one WAN port is configured, proceed to **Configuring Default LAN Settings, page 43**. If two WAN ports are configured, use the Secondary WAN Connection page to configure the secondary WAN connection by using the account information provided by your ISP.

- **WAN Name:** The name of the secondary WAN port.
- **IP Address Assignment:** Depending on the requirements of your ISP, choose the network addressing mode and configure the corresponding fields for the secondary WAN port. For complete details, see Network Addressing Mode, page 125.

STEP 23 After you are finished, click **Next**.

Configuring WAN Redundancy

STEP 24 If you have two WAN links, use the WAN Redundancy page to determine how the two ISP links are used.

- **Equal Load Balancing (Round Robin):** Choose this option if you want to re-order the WAN ports for Round Robin selection. The order is as follows: WAN1 and WAN2. The Round Robin will then be back to WAN1 and continue the order.
- **Weighted Load Balancing:** Choose this option if you want to distribute the bandwidth to two WAN ports by the weighted percentage or by the weighted link bandwidth. The two links will carry data for the protocols that are bound to them.

- **Weighted By Percentage:** If you choose this option, specify the percentage of bandwidth for each WAN, such as 80% for WAN1 and 20% for WAN2.
- **Weighted by Link Bandwidth:** If you choose this option, specify the amount of bandwidth for each WAN, such as 80 Mbps for WAN1 and 20 Mbps for WAN2.

NOTE: The Weighted by Link Bandwidth option has the same effect as the Weighted by Percentage option. However, it provides more percentage options than in the Weighted by Percentage field.

- **Failover:** Choose this option if you want to use one ISP link as a backup. If a failure is detected on the primary link, then the security appliance directs all Internet traffic to the backup link. When the primary link regains connectivity, all Internet traffic is directed to the primary link and the backup link becomes idle.
  - **Select WAN Precedence:** Choose one of the following options:

    Primary: WAN1; Secondary: WAN2: If you choose this option, WAN1 is set as the primary link and WAN2 is set as the backup link.

    Primary: WAN2; Secondary: WAN1: If you choose this option, WAN2 is set as the primary link and WAN1 is set as the backup link.
  - **Preempt Delay Timer:** Enter the time in seconds that the security appliance will preempt the primary link from the backup link after the primary link is up again. The default is 5 seconds.

STEP 25 After you are finished, click **Next**.

Configuring Default LAN Settings

STEP 26 Use the LAN Configuration page to configure the default LAN settings.

- **IP Address:** Enter the subnet IP address for the default LAN.
- **Netmask:** Enter the subnet mask for the default LAN.
- **DHCP Mode:** Choose one of the following DHCP modes:
  - **Disable:** Choose this option if the computers on the LAN are configured with static IP addresses or are configured to use another DHCP server.

- **DHCP Server:** Allows the security appliance to act as a DHCP server and assigns IP addresses to all devices that are connected to the LAN. Any new DHCP client joining the LAN is assigned an IP address of the DHCP pool.
- **DHCP Relay:** Allows the security appliance to use a DHCP Relay. If you choose DHCP Relay, enter the IP address of the remote DHCP server in the **Relay IP** field.

STEP 27 If you choose **DHCP Server** as the DHCP mode, enter the following information:

- **Start IP:** Enter the starting IP address of the DHCP pool.
- **End IP:** Enter the ending IP address of the DHCP pool.

  NOTE: The Start IP address and End IP address should be in the same subnet as the LAN IP address.
- **Lease Time:** Enter the maximum connection time that a dynamic IP address is "leased" to a network user. When the time elapses, the user is automatically renewed the dynamic IP address.
- **DNS1:** Enter the IP address of the primary DNS server.
- **DNS2:** Optionally, enter the IP address of the secondary DNS server.
- **WINS1:** Optionally, enter the IP address of the primary WINS server.
- **WINS2:** Optionally, enter the IP address of the secondary WINS server.
- **Domain Name:** Optionally, enter the domain name for the default LAN.
- **Default Gateway:** Enter the IP address of default gateway.

STEP 28 After you are finished, click **Next**.

Configuring DMZ

STEP 29 If you have not configured a DMZ port, proceed to **Configuring Wireless Radio Settings, page 47**. If you configured a DMZ port, use the DMZ Configuration page to configure a DMZ network.

- **IP Address:** Enter the subnet IP address for the DMZ.
- **Netmask:** Enter the subnet mask for the DMZ.

- **DHCP Mode:** Choose one of the following DHCP modes:
  - **Disable:** Choose this option if the computers on the DMZ are configured with static IP addresses or are configured to use another DHCP server.
  - **DHCP Server:** Allows the security appliance to act as a DHCP server and assigns IP addresses to all devices that are connected to the DMZ. Any new DHCP client joining the DMZ is assigned an IP address of the DHCP pool.
  - **DHCP Relay:** Allows the security appliance to use a DHCP Relay. If you choose DHCP Relay, enter the IP address of the remote DHCP server in the **Relay IP** field.

STEP 30 If you choose **DHCP Server** as the DHCP mode, enter the following information:

- **Start IP:** Enter the starting IP address of the DHCP pool.
- **End IP:** Enter the ending IP address of the DHCP pool.

  NOTE: The Start IP address and End IP address should be in the same subnet with the DMZ IP address.
- **Lease Time:** Enter the maximum connection time that a dynamic IP address is "leased" to a network user. When the time elapses, the user is automatically renewed the dynamic IP address.
- **DNS1:** Enter the IP address of the primary DNS server.
- **DNS2:** Optionally, enter the IP address of the secondary DNS server.
- **WINS1:** Optionally, enter the IP address of the primary WINS server.
- **WINS2:** Optionally, enter the IP address of the secondary WINS server.
- **Domain Name:** Optionally, enter the domain name for the DMZ.
- **Default Gateway:** Enter the IP address of default gateway.

STEP 31 After you are finished, click **Next**.

Configuring DMZ Services

STEP 32 Use the DMZ Service page to configure the DMZ services.

STEP 33 Click **Add** to create a DMZ service.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

STEP 34 In the DMZ Service - Add/Edit window, enter the following information:

- **Original Service:** Choose a service as the incoming service.
- **Translated Service:** Choose a service as the translated service or choose **Original** if the translated service is same as the incoming service. If the service that you want is not in the list, choose **Create a new service** to create a new service object. To maintain the service objects, go to the Networking > Service Management page. See Service Management, page 177.

  NOTE: One-to-one translation will be performed for port range forwarding. For example, if you want to translate an original TCP service with the port range of 50000 to 50002 to a TCP service with the port range of 60000 to 60002, then the port 50000 will be translated to the port 60000, the port 50001 will be translated to the port 60001, and the port 50002 will be translated to the port 60002.
- **Translated IP:** Choose the IP address of your local server that needs to be translated. If the IP address that you want is not in the list, choose **Create a new address** to create a new IP address object. To maintain the IP address objects, go to the Networking > Address Management page. See Address Management, page 175.
- **WAN:** Choose either WAN1 or WAN2, or both as the incoming WAN port.
- **WAN IP:** Specify the public IP address for the server. You can use the IP address of the selected WAN port or a public IP address that is provided by your ISP. When you choose **Both** as the incoming WAN port, this option is grayed out.
- **Enable DMZ Service:** Click **On** to enable the DMZ service, or click **Off** to create only the DMZ service.
- **Create Firewall Rule:** Check this box to automatically create a firewall rule to allow access for this DMZ service. You must manually create a firewall rule if you uncheck this box.

  NOTE: If you choose Both as the incoming WAN port, a firewall rule from Any zone to Any zone will be created accordingly.
- **Description:** Enter the name for the DMZ service.

For example, you host an RDP server (192.168.12.101) on the DMZ. Your ISP has provided a static IP address (172.39.202.102) that you want to expose to the public as your RDP server address. You can create a DMZ service as follows to allow Internet user to access the RDP server by using the specified public IP address.

Original Service	RDP
Translated Service	RDP
Translated IP	RDPServer
WAN	WAN1
WAN IP	PublicIP
Enable DMZ Service	On
Create Firewall Rule	On

NOTE: In this example, you must manually create two address objects (RDPServer and PublicIP) and a TCP service object with the port 3389 called "RDP."

STEP 35 Click **OK** to save your settings.

STEP 36 After you are finished, click **Next**.

Configuring Wireless Radio Settings

STEP 37 If you are using the ISA550 or ISA570, proceed to **Viewing Configuration Summary, page 50**. If you are using the ISA550W or ISA570W, use the Wireless Radio Setting page to configure the wireless radio settings.

- **Wireless Radio:** Click **On** to turn wireless radio on and hence enable the SSID called "cisco-data," or click **Off** to turn wireless radio off.
- **Wireless Network Mode:** Choose the 802.11 modulation technique.
  - **802.11b/g mixed:** Choose this mode if some devices in the wireless network use 802.11b and others use 802.11g. Both 802.11b and 802.11g clients can connect to the access point.
  - **802.11g/n mixed:** Choose this mode if some devices in the wireless network use 802.11g and others use 802.11n Both 802.11g and 802.11n clients can connect to the access point.

- **802.11b/g/n mixed:** Choose this mode to allow 802.11b, 802.11g, and 802.11n clients operating in the 2.4 GHz frequency to connect to the access point.
- **802.11n only:** Choose this mode if all devices in the wireless network can support 802.11n. Only 802.11n clients operating in the 2.4 GHz frequency can connect to the access point.

▪ **Wireless Channel:** Choose a channel from a list of channels or choose **Auto** to let the system determine the optimal channel to use based on the environmental noise levels for the available channels.

STEP 38 After you are finished, click **Next**.

Configuring Intranet WLAN Access

STEP 39 If you turned the wireless radio off, proceed to **Viewing Configuration Summary, page 50**. If you turned the wireless radio on, use the Intranet WLAN Access page to configure the wireless connectivity settings for the SSID called “cisco-data.”

▪ **SSID Name:** The name of the SSID.

▪ **Security Mode:** Choose the encryption algorithm for data encryption for this SSID and configure the corresponding settings. For complete details, see Configuring Wireless Security, page 211.

▪ **VLAN Name:** Choose the VLAN to which this SSID is mapped. All traffic from the wireless clients that are connected to this SSID will be directed to the selected VLAN. For Intranet VLAN access, you must choose a VLAN that is mapped to a trusted zone.

NOTE: ISA550W and ISA570W support four SSIDs. To configure the wireless connectivity settings for other SSIDs, go to the Wireless > Basic Settings page (see Configuring SSID Profiles, page 210), or use the Wireless Wizard (see Using the Wireless Wizard (for ISA550W and ISA570W only), page 76).

STEP 40 After you are finished, click **Next**.

Configure Security Services

STEP 41 Use the Security Services page to enable security services and to specify how to handle the affected traffic when the reputation-based security services are unavailable.

NOTE:

- Enabling a security service will apply its default settings on the security appliance to provide a moderate level of protection. We strongly recommend that you customize the settings for each enabled security service after the Setup Wizard is complete. For complete details, see **Chapter 7, "Security Services."**
- Application Control and Web URL Filtering need additional configuration on the Security Services pages.
- A valid security license is required to activate security services. If the security license is not yet installed, go back the License Installation page to enter the Product Authorization Key (PAK) and email address. After the Setup Wizard is complete, the security appliance first validates the security license through the Internet and then activates security services.

The following features are available:

- **Anti-Virus:** Anti-Virus blocks viruses and malware from entering your network through email, web, FTP, CIFS, and NetBIOS applications. Check this box to enable the Anti-Virus feature on the security appliance, or uncheck this box to disable it.
- **Intrusion Prevention (IPS):** IPS monitors network protocols and prevents attacks to client devices by analyzing and responding to certain types of network traffic. Check this box to enable the IPS feature on the security appliance, or uncheck this box to disable it.
- **Network Reputation:** Network Reputation blocks incoming traffic from IP addresses that are known to initiate attacks throughout the Internet. Check this box to enable the Network Reputation feature on the security appliance, or uncheck this box to disable it. By default, Network Reputation is enabled.
- **Spam Filter:** Spam Filter detects and blocks email spam. Check this box to enable the Spam Filter feature on the security appliance, or uncheck this box to disable it. If you enable Spam Filter, enter the IP address or domain name of your internal SMTP server in the **Local SMTP Server IP Address** field. The SMTP server must have its Internet traffic routed through the security

appliance. The SMTP server or the clients that use this SMTP server can be configured to respond to the spam and suspected spam tags that the security appliance applies to the emails.

- **Web Reputation Filtering:** Web Reputation Filtering prevents client devices from accessing dangerous websites containing viruses, spyware, malware, or phishing links. Check this box to enable the Web Reputation Filtering feature on the security appliance, uncheck this box to disable it.

  NOTE: Clicking the **Details** link for a security service can open the help page that provides complete details for the security service.

STEP 42 Spam Filter, Network Reputation, Web Reputation Filtering, and Web URL Filtering are reputation-based security services. You can specify how to deal with the affected traffic when these reputation services are unavailable. Choose one of the following options:

- **Prevent affected network traffic:** All affected traffic is blocked until the reputation-based security services are available.
- **Allow affected network traffic:** All affected traffic is allowed until the reputation-based security services are available.

STEP 43 After you are finished, click **Next**.

Viewing Configuration Summary

STEP 44 Use the Summary page to view information about the configuration.

STEP 45 To modify any settings, click **Back**. If the configuration is correct, click **Apply** to apply the settings.

After your configuration is successfully applied, the Setup Wizard immediately checks for firmware updates.

STEP 46 If the Firmware Upgrade window appears, follow the on-screen prompts to download and install the firmware. See Upgrading your Firmware After your First Login, page 33. If you are using the latest firmware, click **Finish**.

Using the Dual WAN Wizard to Configure WAN Redundancy Settings

If you have two ISP links, a backup WAN is required so that you can provide backup connectivity or load balancing. Use the Dual WAN Wizard to configure the WAN redundancy settings. Refer to the following steps:

- Starting the Dual WAN Wizard, page 51
- Configuring a Configurable Port as a Secondary WAN Port, page 51
- Configuring the Primary WAN, page 52
- Configuring the Secondary WAN, page 52
- Configuring WAN Redundancy, page 52
- Configuring Network Failure Detection, page 53
- Viewing Configuration Summary, page 54

Starting the Dual WAN Wizard

STEP 1 Click **Configuration Wizards > Dual WAN Wizard**.

STEP 2 Click **Next**.

Configuring a Configurable Port as a Secondary WAN Port

STEP 3 On the Port Configuration page, specify a configurable port (from GE6 to GE10) as the secondary WAN port. The physical port GE1 is reserved for the primary WAN port.

STEP 4 After you are finished, click **Next**.

Configuring the Primary WAN

STEP 5 Use the Primary WAN Connection page to configure the primary WAN connection by using the account information provided by your ISP.

- **WAN Name:** The name of the primary WAN port.
- **IP Address Assignment:** Depending on the requirements of your ISP, choose the network addressing mode and configure the corresponding fields for the primary WAN port. The security appliance supports DHCP Client, Static IP, PPPoE, PPTP, and L2TP. For complete details, see Network Addressing Mode, page 125.

STEP 6 After you are finished, click **Next**.

Configuring the Secondary WAN

STEP 7 Use the Secondary WAN Connection page to configure the secondary WAN connection by using the account information provided by your ISP.

- **WAN Name:** The name of the secondary WAN port.
- **IP Address Assignment:** Depending on the requirements of your ISP, choose the network addressing mode and configure the corresponding fields for the secondary WAN port. For complete details, see Network Addressing Mode, page 125.

STEP 8 After you are finished, click **Next**.

Configuring WAN Redundancy

STEP 9 Use the WAN Redundancy page to determine how the two ISP links are used.

- **Weighted Load Balancing:** Choose this option if you want to use both ISP links simultaneously. Load Balancing distributes the bandwidth to two WAN ports by the weighted percentage or by the weighted link bandwidth. The two links will carry data for the protocols that are bound to them.
  - **Weighted by percentage:** If you choose this option, specify the percentage for each WAN, such as 80% percentage bandwidth for WAN1 and least 20% percentage bandwidth for WAN2.

- **Weighted by Link Bandwidth:** If you choose this option, specify the amount of bandwidth for each WAN, such as 80 Mbps for WAN1 and 20 Mbps for WAN2, which indicates that 80% bandwidth is distributed to WAN1 and at least 20% bandwidth is distributed to WAN2.

NOTE: The Weighted by Link Bandwidth option has the same effect with the Weighted by Percentage option. It just provides more percentage options than Weighted by Percentage that only provides three percentage options.

- **Failover:** Choose this option if you want to use one ISP link as a backup. The Failover mode directs all Internet traffic to the secondary link if the primary link is down. When the primary link regains connectivity, all Internet traffic is directed to the primary link and the secondary link becomes idle.
  - **Select WAN Precedence:** Choose one of the following options:

    Primary: WAN1; Secondary: WAN2: If you choose this option, WAN1 is set as the primary link and WAN2 is set as the backup link.

    Primary: WAN2; Secondary: WAN1: If you choose this option, WAN2 is set as the primary link and WAN1 is set as the backup link.
  - **Preempt Delay Timer:** Enter the time in seconds that the security appliance will preempt the primary link from the backup link after the primary link is up again. The default is 5 seconds.

STEP 10 After you are finished, click **Next**.

Configuring Network Failure Detection

STEP 11 Use the Network Detection page to configure network failure detection.

- **Retry Count:** Enter the number of retries. The security appliance repeatedly tries to connect to the ISP after the network failure is detected.
- **Retry Timeout:** Enter the interval value between two detection packets (Ping or DNS detection).
- **Ping Detection-Ping using WAN Default Gateway:** If you choose this option, ping the IP address of the default WAN gateway. If the default WAN gateway can be detected, the network connection is active.
- **DNS Detection-DNS lookup using WAN DNS Servers:** If you choose this option, the security appliance sends the DNS query for www.cisco.com to the default WAN DNS server. If the DNS server can be detected, the network connection is active.

STEP 12 After you are finished, click **Next**.

Viewing Configuration Summary

STEP 13 Use the Summary page to view information about the configuration.

STEP 14 To modify any settings, click **Back**. If the configuration is correct, click **Finish** to apply your settings.

Using the Remote Access VPN Wizard

Use the Remote Access VPN Wizard to configure the security appliance as an IPsec VPN server or as a SSL VPN gateway so that remote users can securely access the corporate network resources over the VPN tunnels. The Remote Access VPN Wizard supports the following VPN types:

- **IPsec Remote Access:** Enable the IPsec Remote Access feature and hence set the security appliance as an IPsec VPN server. If you choose this option, follow the on-screen prompts to configure an IPsec Remote Access group policy and specify the users and user groups for IPsec remote access. For complete details, see **Using the Remote Access VPN Wizard for IPsec Remote Access, page 54**.
- **SSL Remote Access:** Enable the SSL Remote Access feature and hence set the security appliance as a SSL VPN server. If you choose this option, follow the on-screen prompts to configure the SSL VPN group policies and specify the users and user groups for SSL remote access. For complete details, see **Using Remote Access VPN Wizard for SSL Remote Access, page 60**.

Using the Remote Access VPN Wizard for IPsec Remote Access

This section describes how to use the Remote Access VPN Wizard to configure an IPsec Remote Access group policy and specify the users and user groups for IPsec remote access. Refer to the following steps:

- **Starting the Remote Access VPN Wizard, page 55**
- **Configuring IPsec Remote Access Group Policy, page 55**

- Configuring WAN Settings, page 56
- Configuring Operation Mode, page 56
- Configuring Access Control Settings, page 57
- Configuring DNS and WINS Settings, page 57
- Configuring Backup Servers, page 58
- Configuring Split Tunneling, page 58
- Viewing Group Policy Summary, page 58
- Configuring IPsec Remote Access User Groups, page 59
- Viewing IPsec Remote Access Summary, page 59

Starting the Remote Access VPN Wizard

STEP 1 Click **Configuration Wizards > Remote Access VPN Wizard**.

STEP 2 On the Getting Started page, choose **IPsec Remote Access** from the **VPN Tunnel Type** drop-down list.

STEP 3 Click **Next**.

Configuring IPsec Remote Access Group Policy

STEP 4 Use the IPsec Group Policy page to configure the following parameters of the IPsec Remote Access group policy:

- **Group Name:** Enter the name for the group policy.
- **IKE Authentication Method:** Specify the authentication method.
  - **Pre-shared Key:** Uses a simple, password-based key to authenticate. If you choose this option, enter the desired value that remote VPN clients must provide to establish the VPN connections. The pre-shared key must be entered exactly the same here and on remote VPN clients.
  - **Certificate:** Uses the digital certificate from a third party Certificate Authority (CA) to authenticate. If you choose this option, select a CA certificate as the local certificate from the **Local Certificate** drop-down list and select a CA certificate as the remote certificate from the **Peer Certificate** drop-down list for authentication. The selected remote certificate on the IPsec VPN server must be set as the local certificate on remote VPN clients.

NOTE: You must have valid CA certificates imported on your security appliance before you use the digital certificates to authenticate. Go to the Device Management > Certificate Management page to import the CA certificates. See Managing Certificates for Authentication, page 418.

STEP 5 After you are finished, click **Next**.

Configuring WAN Settings

STEP 6 Use the WAN page to choose the WAN port that traffic passes through over the VPN tunnel. If you have two links, you can enable WAN Failover to redirect traffic to the secondary link when the primary link is down.

- **WAN Failover:** Click **On** to enable WAN Failover, or click **Off** to disable it.

  NOTE: To enable WAN Failover for IPsec Remote Access, make sure that the secondary WAN port was configured and the WAN redundancy was set as the Load Balancing or Failover mode. The security appliance will automatically update the local WAN gateway for the VPN tunnel based on the configurations of the backup WAN link. For this purpose, Dynamic DNS has to be configured because the IP address will change due to failover. In this case, remote VPN clients must use the domain name of the IPsec VPN server to establish the VPN connections.

- **WAN Interface:** Choose the WAN port that traffic passes through over the VPN tunnel.

STEP 7 After you are finished, click **Next**.

Configuring Operation Mode

STEP 8 Use the Network page to configure the mode of operation. The Cisco VPN hardware client supports Network Extension Mode (NEM) and Client Mode. The IPsec Remote Access group policy must be configured with the corresponding mode to allow only the Cisco VPN hardware clients in the same operation mode to be connected.

For example, if you choose the Client mode for the IPsec Remote Access group policy, only the Cisco VPN hardware clients in Client mode can be connected by using this group policy. For more information about the operation mode, see Modes of Operation, page 365.

- **Mode:** Choose one of the following modes:
  - **Client:** Choose this mode for the group policy that is used for both the PC running the Cisco VPN Client software and the Cisco device that supports the Cisco VPN hardware client in Client mode. In Client mode,

the IPsec VPN server can assign the IP addresses to the outside interfaces of remote VPN clients. To define the pool range for remote VPN clients, enter the starting and ending IP addresses in the **Start IP** and **End IP** fields.

- **NEM:** Choose this mode for the group policy that is only used for the Cisco device that supports the Cisco VPN hardware client in NEM mode.

- **Client Internet Access:** Check this box to automatically create advanced NAT rules to allow remote VPN clients to access the Internet over the VPN tunnels. If you uncheck this box, you can manually create advanced NAT rules. For complete details, see Allowing IPsec Remote VPN Clients to Access the Internet, page 360.

STEP 9 After you are finished, click **Next**.

Configuring Access Control Settings

STEP 10 Use the Access Control page to control access from the PC running the Cisco VPN Client software or the private network of the Cisco VPN hardware client to the zones over the VPN tunnel. Click **Permit** to permit access, or click **Deny** to deny access.

NOTE: The VPN firewall rules that are automatically generated by the zone access control settings will be added to the list of firewall rules with the priority higher than the default firewall rules, but lower than the custom firewall rules.

STEP 11 After you are finished, click **Next**.

Configuring DNS and WINS Settings

STEP 12 Optionally, use the DNS/WINS page to specify the DNS and domain settings.

- **Primary DNS Server:** Enter the IP address of the primary DNS server.
- **Secondary DNS Server:** Enter the IP address of the secondary DNS server.
- **Primary WINS Server:** Enter the IP address of the primary WINS server.
- **Secondary WINS Server:** Enter the IP address of the secondary WINS server.
- **Default Domain:** Enter the default domain name that should be pushed to remote VPN clients.

STEP 13 After you are finished, click **Next**.

Configuring Backup Servers

STEP 14 Use the Backup Server page to optionally specify up to three IPsec VPN servers as backup. When the connection to the primary server fails, remote VPN clients can attempt to connect to the backup servers.

Backup Server 1/2/3: Enter the IP address or domain name for the backup server. The backup server 1 has the highest priority and the backup server 3 has the lowest priority.

NOTE: The backup servers that you specified on the IPsec VPN server will be sent to remote VPN clients when initiating the VPN connections. The remote VPN clients will cache them.

STEP 15 After you are finished, click **Next**.

Configuring Split Tunneling

STEP 16 Use the Split Tunnel page to specify the split tunneling settings:

- **Split Tunnel:** Click **On** to enable the split tunneling feature, or click **Off** to disable it. Split tunneling allows only traffic that is specified by the VPN client routes to corporate resources through the VPN tunnel. If you enable the split tunneling feature, you need to define the split subnets. To add a subnet, enter the IP address and netmask in the **IP Address** and **Netmask** fields and click **Add**. To delete a subnet, select it from the list and click **Delete**.
- **Split DNS:** Split DNS directs DNS packets in clear text through the VPN tunnel for domains served by the corporate DNS. To add a domain, enter domain name that should be resolved by your network's DNS server in the **Domain Name** field and click **Add**. To delete a domain, select it from the list and click **Delete**.

  To use Split DNS, you must also enable the split tunneling feature and specify the domains. The Split DNS feature supports up to 10 domains.

STEP 17 After you are finished, click **Next**.

Viewing Group Policy Summary

STEP 18 Use the Group Policy Summary page to view information for the group policy settings.

STEP 19 Click **Next**.

Configuring IPsec Remote Access User Groups

STEP 20 Use the IPsec Remote Access - User Group page to configure the users and user groups for IPsec remote access. The IPsec Remote Access service must be enabled for each user group. All members of the user groups can use the specified group policy to establish the VPN connections.

STEP 21 Click **Add** to add a user group.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

STEP 22 In the **Group Settings** tab, enter the following information:

- **Name:** Enter the name for the user group.
- **Services:** Specify the service policy for the user group. The **IPsec Remote Access** service must be enabled for this user group so that all members of the group can establish the VPN tunnel to securely access your network resources.

STEP 23 In the **Membership** tab, specify the members of the user group. You must add at least one user in the user group before proceeding.

- To add a member, select an existing user from the **User** list and click the right arrow. The members of the group appear in the **Membership** list.
- To delete a member from the group, select the member from the **Membership** list and then click the left arrow.
- To create a new user, enter the username in the **User Name** field and the password in the **Password** field, enter the same password in the **Password Confirm** field for confirmation, and then click **Create**.

STEP 24 Click **OK** to save your settings.

STEP 25 After you are finished, click **Next**.

Viewing IPsec Remote Access Summary

STEP 26 Use the IPsec Remote Access - Summary page to view information for the specified IPsec Remote Access group policy and user groups.

STEP 27 To modify any settings, click **Back**. If the configuration is correct, click **Finish** to apply your settings.

After the settings are saved, the security appliance is set as an IPsec VPN server. Remote users that belong to the specified user groups can use the specified group policy to establish the VPN connections. If you check **Client Internet Access**, the corresponding advanced NAT rules are automatically created to allow remote VPN clients to access the Internet over the VPN tunnels.

Using Remote Access VPN Wizard for SSL Remote Access

This section describes how to use the Remote Access VPN Wizard to configure the SSL VPN group policies and specify the users and user groups for SSL remote access. Refer to the following steps:

- **Starting the Remote Access VPN Wizard with SSL Remote Access, page 60**
- **Configuring SSL VPN Gateway, page 60**
- **Configuring SSL VPN Group Policy, page 62**
- **Configuring SSL VPN User Groups, page 65**
- **Viewing SSL VPN Summary, page 66**

Starting the Remote Access VPN Wizard with SSL Remote Access

STEP 1 Click **Configuration Wizards > Remote Access VPN Wizard**.

STEP 2 Choose **SSL Remote Access** from the **VPN Tunnel Type** drop-down list.

STEP 3 Click **Next**.

Configuring SSL VPN Gateway

STEP 4 Use the SSL VPN - Configuration page to configure the SSL VPN gateway settings.

STEP 5 In the **Gateway (Basic)** area, enter the following information:

- **Gateway Interface:** Choose the WAN port that traffic passes through the SSL VPN tunnel.
- **Gateway Port:** Enter the port number used for the SSL VPN gateway. By default, SSL operates on port 443. However, the SSL VPN gateway should be flexible enough to operate on a user defined port. The firewall should

permit the port to ensure delivery of packets destined for the SSL VPN gateway. The SSL VPN clients need to enter the entire address pair "Gateway IP address: Gateway port number" for connecting purposes.

- **Certificate File:** Choose the default certificate or an imported certificate to authenticate users who try to access your network resource through the SSL VPN tunnels. For information on importing the certificates, see Managing Certificates for Authentication, page 418.
- **Client Address Pool:** The SSL VPN gateway has a configurable address pool with maximum size of 255 which is used to allocate IP addresses to the remote clients. Enter the IP address pool for all remote clients. The client is assigned an IP address by the SSL VPN gateway.

  NOTE: Configure an IP address range that does not directly overlap with any other addresses on your local network.
- **Client Netmask:** Enter the IP address of the netmask used for SSL VPN clients. The client netmask can only be one of 255.255.255.0, 255.255.255.128, and 255.255.255.192.

  The Client Address Pool is used with the Client Netmask. The following table displays the valid settings for entering the client address pool and the client netmask.

Client Netmask	Client Address Pool
255.255.255.0	x.x.x.0
255.255.255.128	x.x.x.0, or x.x.x.128
255.255.255.192	x.x.x.0, x.x.x.64, x.x.x.128, or x.x.x.192

  For example, if they are set as follows, then the SSL VPN client will get a VPN address whose range is from 10.10.10.1 to 10.10.10.254.

  - Client Address Pool = 10.10.10.0
  - Client Netmask = 255.255.255.0
- **Client Internet Access:** Check this box to automatically create advanced NAT rules to allow SSL VPN clients to access the Internet over SSL VPN tunnels. If you uncheck this box, you can manually create advanced NAT rules. For complete details, see Allowing SSL VPN Clients to Access the Internet, page 382.

- **Client Domain:** Enter the domain name that should be pushed to the SSL VPN clients.
- **Login Banner:** After the SSL VPN user logged in, a configurable login banner is displayed. Enter the message text to display along with the banner.

STEP 6 In the **Gateway (Advanced)** area, enter the following information:

- **Idle Timeout:** Enter the timeout value in seconds that the SSL VPN session can remain idle. The default value is 2100 seconds.
- **Session Timeout:** Enter the timeout value in seconds that a SSL VPN session can remain active. The default value is 0 seconds, which indicates that the SSL VPN session can always be active.
- **Client DPD Timeout:** Dead Peer Detection (DPD) allows detection of dead peers. Enter the DPD timeout that a session will be maintained with a nonresponsive remote client. The default value is 300 seconds.
- **Gateway DPD Timeout:** Enter the DPD timeout that a session will be maintained with a nonresponsive SSL VPN gateway. The default value is 300 seconds.

  NOTE: If the SSL VPN gateway has no response over two or three times of the DPD timeout, the SSL VPN session will be terminated.
- **Keep Alive:** Enter the interval, in seconds, at which the SSL VPN client will send keepalive messages. These messages ensure that the SSL VPN connection remains open, even if the client's maximum idle time is limited by an intermediate device, such as a proxy, firewall or NAT device.
- **Lease Duration:** Enter the amount of time after which the SSL VPN client must send an IP address lease renewal request to the server. The default value is 43200 seconds.
- **Max MTU:** Enter the maximum transmission unit for the session. The default value is 1406 bytes.
- **Rekey Interval:** Enter the frequency of the rekey in this field. The default value is 3600 seconds.

STEP 7 After you are finished, click **Next**.

Configuring SSL VPN Group Policy

STEP 8 Use the Group Policy page to configure the SSL VPN group policies.

NOTE: Up to 32 SSL VPN group policies can be configured on the security appliance.

STEP 9 Click **Add** to add a new SSL VPN group policy.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

STEP 10 In the **Basic Settings** tab, enter the following information:

- **Policy Name:** Enter the name for the SSL VPN group policy.
- **Primary DNS:** Optionally, enter the IP address of the primary DNS server.
- **Secondary DNS:** Optionally, enter the IP address of the secondary DNS server.
- **Primary WINS:** Optionally, enter the IP address of the primary WINS server.
- **Secondary WINS:** Optionally, enter the IP address of the secondary WINS server.

STEP 11 In the **IE Proxy Settings** tab, enter the following information:

The SSL VPN gateway can specify several Microsoft Internet Explorer (MSIE) proxies for client PCs. If these settings are enabled, IE on the client PC is automatically configured with these settings.

- **IE Proxy Policy:** Choose one of the following options:
  - **None:** Allows the browser to use no proxy settings.
  - **Auto:** Allows the browser to automatically detect the proxy settings.
  - **Bypass-Local:** Allows the browser to bypass the proxy settings that are configured on the remote user.
  - **Disable:** Disables the MSIE proxy settings.
- **Address:** If you choose Bypass-Local or Auto, enter the IP address or domain name of the MSIE proxy server.
- **Port:** Enter the port number of the MSIE proxy server.
- **IE Proxy Exception:** You can specify the exception hosts for IE proxy settings. This option allows the browser to not send traffic for the given hostname or IP address through the proxy. To add an entry, enter the IP address or domain name of an exception host and click **Add**.

STEP 12 In the **Split Tunneling Settings** area, enter the following information:

Split tunneling permits specific traffic to be carried outside of the SSL VPN tunnel. Traffic is either included (resolved in tunnel) or excluded (resolved through the ISP or WAN connection). Tunnel resolution configuration is mutually exclusive. An IP address cannot be both included and excluded at the same time.

- **Enable Split Tunneling:** By default, all of traffic from the host is directed through the tunnel. Check this box to enable the split tunneling feature so that the tunnel is used only for traffic that is specified by the client routes.
- **Split Selection:** If you enable split tunneling, choose one of the following options:
  - **Include Traffic:** Allows you to add the client routes on the SSL VPN client so that only traffic to the destination networks can be redirected through the SSL VPN tunnels. To add a client route, enter the destination subnet to which a route is added on the SSL VPN client in the **Address** field and the subnet mask for the destination network in the **Netmask** field, and then click **Add**.
  - **Exclude Traffic:** Allows you to exclude the destination networks on the SSL VPN client. Traffic to the destination networks is redirected using the SSL VPN client's native network interface (resolved through the ISP or WAN connection). To add a destination subnet, enter the destination subnet to which a route is excluded on the SSL VPN client in the **Address** field and the subnet mask for the excluded destination in the **Netmask** field, and then click **Add**.

    NOTE: To exclude the destination networks, make sure that the Exclude Local LANs feature is enabled on the Cisco AnyConnect Secure Mobility clients.
  - **Exclude Local LANs:** If you choose Exclude Traffic, check the box to permit remote users to access their local LANs without passing through VPN tunnel, or uncheck the box to deny remote users to access their local LANs without passing through VPN tunnel.

    NOTE: To exclude local LANs, make sure that the Exclude Local LANs feature is enabled on both the SSL VPN server and the Cisco AnyConnect Secure Mobility clients.
- **Split DNS:** Split DNS can direct DNS packets in clear text over the Internet for domains served through an external DNS (serving your ISP) or through a SSL VPN tunnel to domains served by the corporate DNS. To add a domain

for tunneling DNS requests to destinations in the private network, enter the IP address or domain name in the field and click **Add**. To delete a domain, select it from the list and click **Delete**.

STEP 13 In the **Zone-based Firewall Settings** area, you can control access from the SSL VPN clients to the zones over the SSL VPN tunnels. Click **Permit** to permit access, or click **Deny** to deny access.

NOTE: The VPN firewall rules that are automatically generated by the zone-based firewall settings will be added to the list of firewall rules with the priority higher than the default firewall rules, but lower than the custom firewall rules.

STEP 14 Click **OK** to save your settings.

STEP 15 After you are finished, click **Next**.

Configuring SSL VPN User Groups

STEP 16 Use the User Group page to configure the users and user groups for SSL remote access. The SSL VPN service must be enabled for the user groups. All members of a user group can use the selected SSL VPN group policy to establish the SSL VPN connections.

STEP 17 Click **Add** to add a user group.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

STEP 18 In the **Group Settings** tab, enter the following information:

- **Name:** Enter the name for the user group.
- **Services:** Specify the service policy for the user group. The **SSL VPN** service must be enabled for this user group so that all members of the user group can establish the SSL VPN tunnels based on the selected SSL VPN group policy to access your network resources.

STEP 19 In the **Membership** tab, specify the members of the user group. You must add at least one user in the user group before proceeding.

- To add a member, select an existing user from the **User** list and then click the right arrow. The members of the group appear in the **Membership** list.
- To delete a member from the group, select the member from the **Membership** list and then click the left arrow.

- To create a new member, enter the username in the **User Name** field and the password in the **Password** field, enter the same password in the **Password Confirm** field for confirmation, and then click **Create**.

STEP 20 Click **OK** to save your settings.

STEP 21 After you are finished, click **Next**.

Viewing SSL VPN Summary

STEP 22 Use the SSL VPN Summary page to view information for all configured SSL VPN group policies and user groups.

STEP 23 To modify any settings, click **Back**. If the configuration is correct, click **Finish** to apply your settings.

After the settings are saved, the security appliance is set as a SSL VPN server. The SSL VPN users that belong to the specified user groups can use the selected group policies to establish the SSL VPN connections. If you check **Client Internet Access**, the advanced NAT rules will be automatically created to allow SSL VPN clients to access the Internet over SSL VPN tunnels.

Using the Site-to-Site VPN Wizard to Configure Site-to-Site VPN

Use the Site-to-Site VPN Wizard to configure a site-to-site VPN policy to provide a secure connection between two routers that are physically separated. Refer to the following steps:

- Starting the Site-to-Site VPN Wizard, page 67
- Configuring VPN Peer Settings, page 67
- Configuring IKE Policies, page 68
- Configuring Transform Policies, page 69
- Configuring Local and Remote Networks, page 70
- Viewing Configuration Summary, page 70

Starting the Site-to-Site VPN Wizard

STEP 1 Click **Configuration Wizards > Site-to-Site VPN Wizard**.

STEP 2 Click **Next**.

Configuring VPN Peer Settings

STEP 3 Use the VPN Peer Settings page to configure an IPsec VPN policy for establishing the VPN connection with a remote router.

- **Profile Name:** Enter the name for the IPsec VPN policy.
- **WAN Interface:** Choose the WAN port that traffic passes through over the VPN tunnel.
- **Remote Type:** Specify the type of the remote peer:
  - **Static IP:** Choose this option if the remote peer uses a static IP address. Enter the IP address of the remote device in the **Remote Address** field.
  - **Dynamic IP:** Choose this option if the remote peer uses a dynamic IP address.
  - **FQDN (Fully Qualified Domain Name):** Choose this option if you want to use the domain name of the remote network such as vpn.company.com. Enter the domain name of the remote device in the **Remote Address** field.
- **Authentication Method:** Specify the authentication method.
  - **Pre-Shared Key:** Uses a simple, password-based key to authenticate. If you choose this option, enter the desired value that the peer device must provide to establish a connection in the **Key** field. The pre-shared key must be entered exactly the same here and on the remote peer.
  - **Certificate:** Uses the digital certificate from a third party Certificate Authority (CA) to authenticate. If you choose this option, select a CA certificate as the local certificate from the **Local Certificate** drop-down list and select a CA certificate as the remote certificate from the **Remote Certificate** drop-down list. The selected remote certificate on the local gateway must be set as the local certificate on the remote peer.

    NOTE: You must have valid CA certificates imported on your security appliance before you use the digital certificates to authenticate. Go to the Device Management > Certificate Management page to import the CA certificates. See Managing Certificates for Authentication, page 418.

STEP 4 After you are finished, click **Next**.

Configuring IKE Policies

STEP 5 Use the IKE Policies page to configure the IKE policies and to specify an IKE policy for the IPsec VPN policy. You can choose the default or a custom IKE policy.

STEP 6 Click **Add** to add an IKE policy.

Other options: To edit an entry, click **Edit**. To delete an entry, select it and click **Delete**. The default IKE policy (**DefaultIke**) cannot be edited or deleted.

STEP 7 Enter the following information:

- **Name:** Enter the name for the IKE policy.
- **Encryption:** Choose the algorithm used to negotiate the security association. There are four algorithms supported by the security appliance: ESP_3DES, ESP_AES_128, ESP_AES_192, and ESP_AES_256.
- **HASH:** Specify the authentication algorithm for the VPN header. There are two HASH algorithms supported by the security appliance: SHA1 and MD5. Ensure that the authentication algorithm is configured identically on both sides.
- **Authentication:** Specify the authentication method that the security appliance uses to establish the identity of each IPsec peer.
  - **PRE_SHARE:** Use a simple, password-based key to authenticate. The alpha-numeric key is shared with IKE peer. Pre-shared keys do not scale well with a growing network but are easier to set up in a small network.
  - **RSA_SIG:** Use a digital certificate to authenticate. RSA_SIG is a digital certificate with keys generated by the RSA signatures algorithm. In this case, a certificate must be configured in order for the RSA-Signature to work.
- **D-H Group:** Choose the Diffie-Hellman group identifier. The identifier is used by two IPsec peers to derive a shared secret without transmitting it to each other. The D-H Group sets the strength of the algorithm in bits. The default is Group 5. The lower the Diffie-Hellman group number, the less CPU time it requires to be executed. The higher the D-H group number, the greater the security level.
  - Group 2 (1024-bit)
  - Group 5 (1536-bit)

- Group 14 (2048-bit)

- **Lifetime:** Enter the number of seconds for the IKE Security Association (SA) to remain valid. As a general rule, a shorter lifetime provides more secure ISAKMP negotiations. However, with shorter lifetimes, the security appliance sets up future IKE SAs more quickly.

STEP 8 Click **OK** to save your settings.

STEP 9 After you are finished, click **Next**.

Configuring Transform Policies

STEP 10 Use the Transform Policies page to configure the transform policies and to specify a transform set for the IPsec VPN policy. You can choose the default or a custom transform set.

STEP 11 Click **Add** to add a transform set.

Other options: To edit an entry, click **Edit**. To delete an entry, select it and click **Delete**. The default transform set (**DefaultTrans**) cannot be edited or deleted.

STEP 12 Enter the following information:

- **Name:** Enter the name for the transform set.
- **Integrity:** Choose the hash algorithm used to ensure data integrity. The hash algorithm ensures that a packet comes from where it says it comes from, and that it has not been modified in transit.
  - **ESP_SHA1_HMAC:** Authentication with SHA1 (160-bit).
  - **ESP_MD5_HMAC:** Authentication with MD5 (128-bit). MD5 has a smaller digest and is considered to be slightly faster than SHA1. A successful (but extremely difficult) attack against MD5 has occurred; however, the HMAC variant that IKE uses prevents this attack.
- **Encryption:** Choose the symmetric encryption algorithm that protects data transmission between two IPsec peers. The default is ESP_3DES. The Advanced Encryption Standard supports key lengths of 128, 192, 256 bits.
  - **ESP_3DES:** Encryption with 3DES (168-bit).
  - **ESP_AES_128:** Encryption with AES (128-bit).
  - **ESP_AES_192:** Encryption with AES (192-bit).
  - **ESP_AES_256:** Encryption with AES (256-bit).

STEP 13 Click **OK** to save your settings.

STEP 14 After you are finished, click **Next**.

Configuring Local and Remote Networks

STEP 15 Use the Local and Remote VPN Networks page to configure the local and remote networks.

- **Local Subnet:** Choose the IP address for your local network. Choose **Any** if you want to enable the zone access control settings so that you can control incoming traffic from remote VPN network to the zones over the VPN tunnels.
- **Remote Subnet:** Choose the IP address for the remote network. You must know the IP address of the remote network before connecting the VPN tunnel.

  If the IP address object that you want is not in the list, choose **Create a new address** to add a new address object or choose **Create a new address group** to add a new address group object. To maintain the address and address group objects, go to the Networking > Address Management page. See Address Management, page 175.

  NOTE: The security appliance can support multiple subnets for establishing the VPN tunnels. You should select an address group object including multiple subnets for local and remote networks.

STEP 16 After you are finished, click **Next**.

Viewing Configuration Summary

STEP 17 Use the Summary page to view information for the IPsec VPN policy.

STEP 18 To modify any settings, click **Back**. If the configuration is correct, click **Finish** to apply your settings.

STEP 19 After you click Finish, a warning message appears saying “Do you want to make this connection active when the settings are saved? (Only one connection can be active at a time.)”

- If you want to immediately activate the connection after the settings are saved, click **Activate Connection**. After you save your settings, the security appliance will immediately try to initiate the VPN connection.

- If you only want to create the IPsec VPN policy and do not want to immediately activate the connection after the settings are saved, click **Do Not Activate**. The connection will be triggered by any traffic that matches this IPsec VPN policy and the VPN tunnel will be set up automatically. You can also go to the VPN > Site-to-Site > IPsec Policies page to manually establish the VPN connection by clicking the **Connect** icon.

Using the DMZ Wizard to Configure DMZ Settings

Use the DMZ Wizard to configure DMZ and DMZ services if you need to host public services. Refer to the following steps:

- Starting the DMZ Wizard, page 71
- Configuring DDNS Profiles, page 71
- Configuring DMZ Network, page 72
- Configuring DMZ Services, page 74
- Viewing Configuration Summary, page 76

Starting the DMZ Wizard

STEP 1 Click **Configuration Wizards > DMZ Wizard**.

STEP 2 Click **Next**.

Configuring DDNS Profiles

STEP 3 Optionally, use the DDNS Setup page to configure the DDNS profiles for remote management of the DMZ network.

NOTE: Up to 16 DDNS profiles can be configured on the security appliance.

STEP 4 Click **Add** to create a DDNS profile.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon.

STEP 5 Enter the following information:

- **Service:** Choose either DynDNS or No-IP service.

  NOTE: You must sign up for an account with either one of these providers before you can use this service.

- **Active On Startup:** Click **On** to activate the DDNS setting when the security appliance starts up.

- **WAN Interface:** Choose the WAN port for the DDNS service. Traffic for DDNS services will pass through the specified WAN port.

  NOTE: If the WAN redundancy is set as the Failover mode, this option is grayed out. When WAN failover occurs, DDNS will switch traffic to the active WAN port.

- **User Name:** Enter the username of the account that you registered in the DDNS provider.

- **Password:** Enter the password of the account that you registered in the DDNS provider.

- **Host and Domain Name:** Specify the complete host name and domain name for the DDNS service.

- **Use wildcards:** Check this box to allow all sub-domains of your DDNS host name to share the same public IP address as the host name.

- **Update every week:** Check this box to update the host information every week.

STEP 6 Click **OK** to save your settings.

STEP 7 After you are finished, click **Next**.

Configuring DMZ Network

STEP 8 Use the DMZ Configuration page to configure the DMZ networks.

NOTE: Up to 4 DMZ networks can be configured on the security appliance. You must configure at least one DMZ network to finish the DMZ wizard.

STEP 9 Click **Add** to create a DMZ network.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon.

STEP 10 In the **Basic Setting** tab, enter the following information:

- **Name:** Enter the name for the DMZ.
- **IP:** Enter the subnet IP address for the DMZ.
- **Netmask:** Enter the subnet mask for the DMZ.
- **Spanning Tree:** Check this box to enable the Spanning Tree feature to determine if there are loops in the network topology.
- **Port:** Choose a configurable port from the **Port** list and add it to the **Member** list. The selected configurable port is set as a DMZ port in the Access mode.
- **Zone:** Choose the default DMZ zone or a custom DMZ zone to which the DMZ is mapped.

STEP 11 In the **DHCP Pool Settings** tab, choose the DHCP mode from the **DHCP Mode** drop-down list.

- **Disable:** Choose this option if the computers on the DMZ are configured with static IP addresses or are configured to use another DHCP server.
- **DHCP Server:** Allows the security appliance to act as a DHCP server and assigns IP addresses to all devices that are connected to the DMZ. Any new DHCP client joining the DMZ is assigned an IP address of the DHCP pool.
- **DHCP Relay:** Allows the security appliance to use a DHCP Relay. If you choose DHCP Relay, enter the IP address of the remote DHCP server in the **Relay IP** field.

STEP 12 If you choose **DHCP Server** as the DHCP mode, enter the following information:

- **Start IP:** Enter the starting IP address of the DHCP pool.
- **End IP:** Enter the ending IP address of the DHCP pool.

  NOTE: The Start IP address and End IP address should be in the same subnet with the DMZ IP address.
- **Lease Time:** Enter the maximum connection time that a dynamic IP address is “leased” to a network user. When the time elapses, the user is automatically assigned a new dynamic IP address.
- **DNS1:** Enter the IP address of the primary DNS server.
- **DNS2:** Optionally, enter the IP address of a secondary DNS server.
- **WINS1:** Optionally, enter the IP address of the primary WINS server.

- **WINS2:** Optionally, enter the IP address of a secondary WINS server.
- **Domain Name:** Optionally, enter the domain name for the DMZ.
- **Default Gateway:** Enter the IP address of default gateway.

STEP 13 Click **OK** to save your settings.

STEP 14 After you are finished, click **Next**.

Configuring DMZ Services

STEP 15 Use the DMZ Service page to configure the DMZ services.

STEP 16 Click **Add** to create a DMZ service.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

STEP 17 Enter the following information:

- **Original Service:** Choose a service as the incoming service.
- **Translated Service:** Choose a service as the translated service or choose **Original** if the translated service is same as the incoming service. If the service that you want is not in the list, choose **Create a new service** to create a new service object. To maintain the service objects, go to the Networking > Service Management page. See Service Management, page 177.

  NOTE: One-to-one translation will be performed for port range forwarding. For example, if you want to translate an original TCP service with the port range of 50000 to 50002 to a TCP service with the port range of 60000 to 60002, then the port 50000 will be translated to the port 60000, the port 50001 will be translated to the port 60001, and the port 50002 will be translated to the port 60002.
- **Translated IP:** Choose the IP address of your local server that needs to be translated. If the IP address that you want is not in the list, choose **Create a new address** to create a new IP address object. To maintain the IP address objects, go to the Networking > Address Management page. See Address Management, page 175.
- **WAN:** Choose either WAN1 or WAN2, or both as the incoming WAN port.

- **WAN IP:** Specify the public IP address for the server. You can use the IP address of the selected WAN port or a public IP address that is provided by your ISP. When you choose **Both** as the incoming WAN port, this option is grayed out.
- **Enable DMZ Service:** Click **On** to enable the DMZ service, or click **Off** to create only the DMZ service.
- **Create Firewall Rule:** Check this box to automatically create a firewall rule to allow access for this DMZ service. You must manually create a firewall rule if you uncheck this box.

  NOTE: If you choose Both as the incoming WAN port, a firewall rule from Any zone to Any zone will be created accordingly.
- **Description:** Enter the name for the DMZ service.

  For example, you host an RDP server (192.168.12.101) on the DMZ. Your ISP has provided a static IP address (172.39.202.102) that you want to expose to the public as your RDP server address. You can create a DMZ service as follows to allow Internet user to access the RDP server by using the specified public IP address.

Original Service	RDP
Translated Service	RDP
Translated IP	RDPServer
WAN	WAN1
WAN IP	PublicIP
Enable DMZ Service	On
Create Firewall Rule	On

NOTE: In the above example, you must manually create two address objects (RDPServer and PublicIP) and a TCP service object with the port 3389 called “RDP.”

STEP 18 Click **OK** to save your settings.

STEP 19 After you are finished, click **Next**.

Viewing Configuration Summary

STEP 20 Use the Summary page to view information for the configuration.

STEP 21 To modify any settings, click **Back**. If the configuration is correct, click **Finish** to apply your settings.

Using the Wireless Wizard (for ISA550W and ISA570W only)

If you are using the ISA550W or ISA570W, you can use the Wireless Wizard to configure your wireless network. Refer to the following steps:

- Starting the Wireless Wizard, page 76
- Configuring Wireless Radio Settings, page 76
- Configuring Wireless Connectivity Types, page 77
- Specify Wireless Connectivity Settings for All Enabled SSIDs, page 78
- Viewing Configuration Summary, page 78

Starting the Wireless Wizard

STEP 1 Click **Configuration Wizards > Wireless Wizard**.

STEP 2 Click **Next**.

Configuring Wireless Radio Settings

STEP 3 Use the Wireless Radio page to configure the wireless radio settings.

- **Wireless Mode:** Choose the 802.11 modulation technique.
  - **802.11b/g mixed:** Choose this mode if some devices in the wireless network use 802.11b and others use 802.11g. Both 802.11b and 802.11g clients can connect to the access point.
  - **802.11g/n mixed:** Choose this mode if some devices in the wireless network use 802.11g and others use 802.11n Both 802.11g and 802.11n clients can connect to the access point.

- **802.11b/g/n mixed:** Choose this mode to allow 802.11b, 802.11g, and 802.11n clients operating in the 2.4 GHz frequency to connect to the access point.
- **802.11n only:** Choose this mode if all devices in the wireless network can support 802.11n. Only 802.11n clients operating in the 2.4 GHz frequency can connect to the access point.

▪ **Wireless Channel:** Choose a channel from a list of channels or choose **Auto** to let the system determine the optimal channel to use based on the environmental noise levels for the available channels.

STEP 4 After you are finished, click **Next**.

Configuring Wireless Connectivity Types

STEP 5 Use the Choose SSIDs page to enable and configure the SSIDs that you want to use.

▪ **Enable:** Check this box to enable the SSID.

▪ **Mode:** Choose the wireless connectivity type for each enabled SSID.

- **Intranet WLAN Access:** Allows the wireless users to access the corporate network via the wireless network. By default, the WLAN is mapped to the DEFAULT VLAN.
- **Guest WLAN Access:** Only allows the wireless users who connect to the guest SSID to access the corporate network via the wireless network. By default, the WLAN is mapped to the GUEST VLAN.
- **Captive Portal Access:** Only allows the users who have authenticated successfully to access the corporate network via the wireless network. The wireless users will be directed to a specific HotSpot Login page to authenticate, and then will be directed to a specified web portal after login before they can access the Internet.

NOTE: Only one SSID can be set for Captive Portal access at a time.

STEP 6 After you are finished, click **Next**.

Specify Wireless Connectivity Settings for All Enabled SSIDs

STEP 7 Specify the wireless connectivity settings for all enabled SSIDs.

- For complete details to configure the connectivity settings for Intranet WLAN access, see **Configuring the SSID for Intranet WLAN Access, page 78**.
- For complete details to configure the connectivity settings for Guest WLAN access, see **Configuring the SSID for Guest WLAN Access, page 80**.

STEP 8 After you are finished, click **Next**.

Viewing Configuration Summary

STEP 9 Use the Summary page to view information for the configuration.

STEP 10 To modify any settings, click **Back**. If the configuration is correct, click **Finish** to save your settings.

Configuring the SSID for Intranet WLAN Access

Follow these steps to configure the connectivity settings for Intranet WLAN access.

STEP 1 Enter the following information:

- **SSID:** Enter the name of the SSID.
- **Broadcast SSID:** Check this box to broadcast the SSID in its beacon frames. All wireless devices within range are able to see the SSID when they scan for available networks. Uncheck this box to prevent auto-detection of the SSID. In this case, users must know the SSID to set up a wireless connection to this SSID.
- **Station Isolation:** Check so that the wireless clients on the same SSID will be unable to see each other.

STEP 2 In the **Security Settings** area, specify the wireless security settings.

- **Security Mode:** Choose the security mode and configure the corresponding security settings. For security purposes, we strongly recommend that you use WPA2 for wireless security. For example, if you choose WPA2-Personal, enter the following information:
  - **Encryption:** WPA2-Personal always uses AES for data encryption.
  - **Shared Secret:** The Pre-shared Key (PSK) is the shared secret key for WPA. Enter a string of at least 8 characters to a maximum of 63 characters.
  - **Key Renewal Timeout:** Enter a value to set the interval at which the key is refreshed for clients associated to this SSID. A value of zero (0) indicates that the key is not refreshed. The default is 3600 seconds.

  NOTE: For information on configuring other security modes, see **Configuring Wireless Security, page 211**.

STEP 3 In the **Advanced Settings** area, enter the following information:

- **VLAN Mapping:** Choose the VLAN to which the SSID is mapped. All traffic from the wireless clients that are connected to this SSID will be directed to the selected VLAN. For Intranet VLAN access, you must choose a VLAN that is mapped to a trusted zone.
- **User Limit:** Specify the maximum number of users that can simultaneously connect to this SSID. Enter a value in the range of 0 to 200. The default value is zero (0), which indicates that there is no limit for this SSID.

  NOTE: The maximum number of users that can simultaneously connect to all enabled SSIDs is 200.

Configuring the SSID for Guest WLAN Access

Follow these steps to configure the connectivity settings for Guest WLAN access.

STEP 1 Enter the following information:

- **SSID:** Enter the name of the SSID.
- **Broadcast SSID:** Check this box to broadcast the SSID in its beacon frames. All wireless devices within range are able to see the SSID when they scan for available networks. Uncheck this box to prevent auto-detection of the SSID. In this case, users must know the SSID to set up a wireless connection to this SSID.
- **Station Isolation:** Check so that the wireless clients on the same SSID will be unable to see each other.

STEP 2 In the **Security Settings** area, specify the wireless security settings.

- **Security Mode:** Choose the security mode and configure the corresponding security settings. For complete details on configuring the security mode, see Configuring Wireless Security, page 211.

STEP 3 In the **Advanced Settings** area, enter the following information:

- **VLAN Mapping:** Choose the VLAN to which the SSID is mapped. All traffic from the wireless clients that are connected to this SSID will be directed to the selected VLAN. For Guest VLAN access, you must choose a VLAN that is mapped to a guest zone.
- **User Limit:** Specify the maximum number of users that can simultaneously connect to this SSID. Enter a value in the range of 0 to 200. The default value is zero (0), which indicates that there is no limit for this SSID.

  NOTE: The maximum number of users that can simultaneously connect to all enabled SSIDs is 200.

3

Status

This chapter describes how to view the status of your security appliance. It includes the following sections:

- Device Status Dashboard, page 84
- Network Status, page 88
- Wireless Status (for ISA550W and ISA570W only), page 99
- NAT Status, page 100
- VPN Status, page 101
- Active User Sessions, page 105
- Security Services Reports, page 106
- System Status, page 112

To access the Status pages, click **Status** in the left hand navigation pane.

Device Status Dashboard

Use the Status > Dashboard page to view information about the security appliance and its current settings.

Status > Dashboard

Field	Description
System Information	
System Name	Unit name of the device.

Field	Description
Firmware (Primary/Secondary)	Firmware version that the security appliance is currently using (Primary), and the firmware version that was previously running (Secondary). By default, the security appliance boots with the primary firmware.
Bootloader Version	Bootloader version of the security appliance.
Serial Number	Serial number of the security appliance.
PID	Product Identifier (PID) of the security appliance, also known as product name, model name, and product number.
UDI	Unique Device Identifier (UDI) of the security appliance. UDI is Cisco's product identification standard for hardware products.
Resource Utilization To see complete details for resource utilization, click **details**.	
CPU Utilization	Current CPU usage.
CPU Utilization Over 1 Minute	Average CPU usage in last one minute.
Memory Utilization	Total memory usage after the security appliance boots.
System Up Time	Duration for which the security appliance has been running.
Current Time	The current date and system time.
Licenses Displays the status of the security license that is used to activate security services. To manage the security license, click **manage**.	
Syslog Summary Displays the summary of the system event logs. Syslog entries can be of different severity levels. To see complete logs, click **details**.	
Emergency	Total number of Emergency logs. Click the number link for complete details.

Field	Description
Alert	Total number of Alert logs. Click the number link for complete details.
Critical	Total number of Critical logs. Click the number link for complete details.
Error	Total number of Error logs. Click the number link for complete details.
Warning	Total number of Warning logs. Click the number link for complete details.
Notification	Total number of Notification logs. Click the number link for complete details.
Information	Total number of Information logs. Click the number link for complete details.
Debug	Total number of Debug logs. Click the number link for complete details.
Site-to-Site VPN	
Displays the total number of active site-to-site VPN tunnels. To see complete details, click **details**.	
Remote Access VPN	
SSL Users	Total number of active SSL VPN users. Click the **SSL Users** link for complete details.
IPsec Users	Total number of active IPsec VPN users. Click the **IPsec Users** link for complete details. This option is only available when the security appliance is acting as an IPsec VPN server.
Routing Mode	
Displays the routing mode (NAT or Routing) between WAN and LAN. By default, the NAT mode is enabled. To enable or disable the Routing mode, click **details**.	
Physical Ports	
Name	Name of the physical port.
Port Type	Type of the physical port, such as WAN, LAN, or DMZ.

Field	Description
Mode	Link status of the physical port.
WAN Mode Displays the WAN operation mode, such as Single - WAN1, Failover, or Load Balancing. To see complete details for WAN redundancy, click **details.**	
WAN Interface(s) To see complete details for all WAN ports, click **details.**	
Name	Name of the WAN port.
IP Address	IP address for the WAN port.
LAN Interfaces To see complete details for all VLANs, click **details.**	
Index	ID of the VLAN.
Name	Name of the VLAN.
DHCP Mode	DHCP mode of the VLAN.
IP Address	Subnet IP address of the VLAN.
DMZ Interface To see complete details for all DMZs, click **details.**	
Port	Configurable port that is set as the DMZ port.
Name	Name of the DMZ port.
IP Address	Subnet IP address of the DMZ port.
Wireless Interfaces (for ISA550W and ISA570W only) To see complete details for all SSIDs, click **details.**	
SSID Number	Number of the SSID.
SSID Name	Name of the SSID.
VLAN	VLANs to which the SSID is mapped.
Client List	Number of client stations that are connected to the SSID.

Network Status

Use the Network Status pages to view information for the various interfaces, the network usage reports, the WAN bandwidth reports, all ARP (Address Resolution Protocol) entries, and DHCP address assignment. Refer to the following topics:

- Status Summary, page 88
- Traffic Statistics, page 91
- Usage Reports, page 92
- WAN Bandwidth Reports, page 94
- ARP Table, page 95
- DHCP Bindings, page 95
- STP Status, page 96
- CDP Neighbor, page 98

Status Summary

Use the Status Summary page to view information for the various interfaces.

Status Summary

Field	Description
Ethernet	
Port	Number of the physical port.
Name	Name of the physical port.
Enable	Shows if the physical port is enabled or disabled.
Port Type	Type of the physical port, such as WAN, LAN, or DMZ.
Line Status	Shows if the physical port is connected or not.
Speed/Duplex	Duplex mode (speed and duplex setting) of the physical port.
Mode	Access mode of the physical port. A WAN or DMZ port is always set to Access mode and a LAN port can be set to Access or Trunk mode.

Field	Description
VLAN	VLANs to which the physical port is mapped.
PVID	The Port VLAN ID (PVID) to be used to forward or filter the untagged packets coming into the port. The PVID of a Trunk port is fixed to the DEFAULT VLAN (1).
WAN	
Name	Name of the WAN port.
WAN Type	Network addressing mode used to connect to the Internet for the WAN port.
Connection Time	Time that the WAN port is connected, in seconds.
Connection Status	Shows if the WAN port obtains an IP address successfully or not. If yes, the connection status shows "Connected."
WAN State	Shows if the WAN port is active or inactive for routing. If the WAN port is active for routing, the WAN state shows "Up." If the WAN port is inactive for routing, the WAN state shows "Down." **NOTE:** The state "Down" means that the network detection fails. Even though the WAN state is down due to network detection failure, the WAN services (like SSL VPN and Remote Administration) can still be connected except the IPsec VPN Access service.
MAC Address	MAC address of the WAN port.
IP Address	IP address of the WAN port that is accessible from the Internet.
Subnet Mask/Prefix Length	Subnet mask or IPv6 prefix length for the WAN port.
Gateway	Default gateway for the WAN port.
DNS Server	DNS server for the WAN port.
Physical Port	Physical port that is associated with the WAN port.

Field	Description
Line Status	Shows if the cable is inserted to the WAN port or not. If the line status shows “Not Connected,” the cable may be loose or malfunctioning, or be plugged out. **NOTE:** If the line status shows “Not Connected,” the Connection Status will show “Not Connected” and the WAN State will show “Down.”
Zone	Zone to which the WAN port is assigned.
VLAN	
LAN MAC Address	MAC address of the default LAN.
Name	Name of the VLAN.
VID	ID of the VLAN.
IP Address	Subnet IP address of the VLAN.
Subnet Mask/Prefix Length	Subnet mask or IPv6 prefix length of the VLAN.
Physical Port	Physical ports that are assigned to the VLAN.
Zone	Zone to which the VLAN is mapped.
DMZ	
Physical Port	Physical port that is assigned to the DMZ.
Zone	Zone to which the DMZ is mapped.
Name	Name of the DMZ.
VID	ID of the VLAN.
IP Address	Subnet IP address of the DMZ.
Subnet Mask/Prefix Length	Subnet mask or IPv6 prefix length of the DMZ.

Traffic Statistics

Use the Traffic Statistics page to view traffic data for the various interfaces. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data. Click **Reset** to reset the values in the Ethernet table to zero.

Traffic Statistics

Field	Description
Ethernet	
Port	Name of the physical port.
Link Status	Shows if the port is connected or not.
Tx Packets	Number of IP packets transmitted by the port.
Rx Packets	Number of IP packets received by the port.
Collisions	Number of signal collisions that have occurred on this port. A collision occurs when the port tries to send data at the same time as a port on the other router or computer that is connected to this port.
Tx Bytes/Sec	Number of bytes transmitted by the port per second.
Rx Bytes/Sec	Number of bytes received by the port per second.
Uptime	Time that the port has been active. The uptime is reset to zero when the security appliance or the port is restarted.
WAN	
Name	Name of the WAN port.
Tx Packets	Number of IP packets transmitted by the WAN port.
Rx Packets	Number of IP packets received by the WAN port.
Collisions	Number of signal collisions that have occurred on this WAN port.
Tx Bytes/Sec	Number of bytes transmitted by the WAN port per second.
Rx Bytes/Sec	Number of bytes received by the WAN port per second.

Field	Description
Uptime	Time that the WAN port has been active. The uptime is reset to zero when the security appliance or the WAN port is restarted.
VLAN	
Name	Name of the VLAN.
Tx Packets	Number of IP packets transmitted by the VLAN.
Rx Packets	Number of IP packets received by the VLAN.
Collisions	Number of signal collisions that have occurred on this VLAN.
Tx Bytes/Sec	Number of bytes transmitted by the VLAN per second.
Rx Bytes/Sec	Number of bytes received by the VLAN per second.
Uptime	Time that the LAN port has been active.
DMZ	
Name	Name of the DMZ.
Tx Packets	Number of IP packets transmitted by the DMZ.
Rx Packets	Number of IP packets received by the DMZ.
Collisions	Number of signal collisions that occurred on the DMZ.
Tx Bytes/Sec	Number of bytes transmitted by the DMZ per second.
Rx Bytes/Sec	Number of bytes received by the DMZ per second.
Uptime	Time that the DMZ port has been active.

Usage Reports

Use the Usage Reports page to view the top 25 websites that have been most frequently visited, the top 25 users of Internet bandwidth by IP address, and the top 25 services and applications that consume the most bandwidth.

STEP 1 In the **Data Collection** area, enter the following information:

- **Enable Bandwidth Usage Report by IP Address:** Check this box to enable the bandwidth usage report sorted by the top 25 IP addresses that consume the most bandwidth.
- **Enable Bandwidth Usage Report by Internet Service:** Check this box to enable the bandwidth usage report sorted by the top 25 services and applications that consume the most bandwidth.
- **Enable Website Visits Report:** Check this box to enable the website visits report sorted by the top 25 URLs that have been most frequently visited.

STEP 2 Click **Save** to save your settings.

STEP 3 In the **Statistics Report** area, choose the desired report from the **Type** drop-down list to view.

- **Bandwidth Usage by IP Address:** This report displays the IP address of the top 25 users who consume the most bandwidth and the sum of bytes received and transmitted per IP address.
- **Bandwidth Usage by Internet Service:** This report displays the following information for the top 25 services and applications that consume the most bandwidth:
  - **Application:** The name for an known service or application or the port number for an unknown service or application. For example, if SMTP (6, 25) is displayed, SMTP is the service name, 6 is the protocol number, and 25 is the port number of the service.
  - **Sessions:** The total number of sessions for the service or application.
  - **Total Bandwidth (TX/RX):** The total number of bytes received and transmitted by the service or application during the period.
  - **Average Bandwidth (TX/RX):** The average number of bytes received and transmitted per second.

  This report is helpful to determine whether the services and applications being used are appropriate for your organization. You can block the services and applications that are consuming a large portion of available bandwidth. For information on blocking the applications, see Configuring Application Control, page 309.
- **Website Visits:** This report displays the URLs of the top 25 websites that have been most frequently visited and the number of hits to each website.

This report only monitors the website visits through the HTTP port specified in the advanced settings of either Firewall Content Filtering or Web URL Filtering. You can block the websites if inappropriate websites appear in this report. For information on blocking the websites, see Configuring Content Filtering to Control Internet Access, page 281, or Configuring Web URL Filtering, page 327.

STEP 4 Click **Refresh** to update the data on the screen, or click **Reset** to reset the values to zero.

- **Statistics Start Time:** Displays the time that the report starts collecting the data.

  NOTE: When a report is enabled or disabled or if you click **Reset**, the sample period for the report is reset.

- **Last Refresh Time:** Displays the time of your last refresh operation.

WAN Bandwidth Reports

Use the WAN Bandwidth page to view the real-time WAN network bandwidth usage per hour in the past 24 hours. This page is automatically updated every 10 seconds.

STEP 1 To enable the WAN bandwidth reports, check the box next to **Collect and Display WAN Bandwidth Statistics**.

STEP 2 Click **Save** to save your settings.

STEP 3 In the **Primary WAN** tab, you can see the real-time network bandwidth usage per hour in the past 24 hours for the primary WAN port.

STEP 4 In the **Secondary WAN** tab, you can see the real-time network bandwidth usage per hour in the past 24 hours for the secondary WAN port if a secondary WAN port is configured.

STEP 5 Click **Refresh** to manually refresh the data.

STEP 6 Click **Reset** to reset the WAN bandwidth usage data for both the primary WAN and the secondary WAN ports.

ARP Table

Address Resolution Protocol (ARP) is a computer-networking protocol that determines a network host's Link Layer or hardware address when only the Internet Layer (IP) or Network Layer address is known.

Use the ARP Table page to view information for all ARP entries. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

ARP Table

Field	Description
IP Address	IP address of the device.
Flag	Flag type of the device.
MAC Address	MAC address of the device, which is associated with the IP address.
Device	Device interface type.

DHCP Bindings

Use the DHCP Bindings page to view information for DHCP address assignment. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

DHCP Bindings

Field	Description
IP Address	IP address assigned to the host or the remote device.
MAC Address	MAC address of the host or the remote device.
Lease Start Time	The lease starting time of the IP address.
Lease End Time	The lease ending time of the IP address.

STP Status

Use the STP Status page to view information about VLANs that have Spanning Tree Protocol (STP) enabled. STP is a Link Layer network protocol that ensures a loop-free topology for any bridged LAN. No information is displayed for VLANs without STP enabled.

At the top of the page, use the **Check the STP status in this VLAN** list to choose a VLAN.

STP Status > Global Status

Field	Description
Bridge ID	An unique ID for the other devices on the network to identify this device.
Root Bridge ID	The bridge ID of the root bridge.
Root Port	The Port ID of the root port. The root port is the port with the lowest path cost to the root bridge. The root bridge does not have a root port.
Root Path Cost	The cost of the shortest path from the security appliance to the root bridge. The value 0 indicates that this security appliance is the root bridge.

Interface Status Table

Field	Description
Interface	The interface name.

Field	Description
Port Role	The role assigned to this port ▪ Root port: The port with the lowest path cost to the root bridge. ▪ Designated port: The port with the lowest path cost on a LAN segment. The LAN segment will use the designated port to reach the root bridge. ▪ Blocked port: The port that is neither a root port nor a designated port.
Path Cost	The cost of the path to root bridge through this port.
Priority	Priority of the port.
Port State	The state of the port: ▪ Disabled: This port is disabled. It will not transmit or receive any traffic. ▪ Blocking: This port is enabled but blocked by STP. It will not transmit or receive any traffic. ▪ Listening: This port will receive and process STP bridge protocol data units (BPDUs), but will not forward any data traffic. ▪ Learning: This port will start to learn MAC addresses from the received packets. It will also receive and process STP BPDUs, but will not forward any data traffic. ▪ Forwarding: This port will forward data traffic, process BPDUs and learn MAC address.
Designated Bridge ID	The ID of the designated bridge of the LAN segment. The designated bridge is used by all the other devices on the LAN segment to reach the root bridge.
Designated Port ID	The ID of the designated port of the LAN segment. The designated port is the port used by all the other devices on the LAN segment to reach the root bridge.

Field	Description
Designated Cost	The path cost to the designated bridge of the LAN segment.

CDP Neighbor

Use the CDP Neighbors page to view status information about neighboring devices that were discovered by the Cisco Discovery Protocol (if enabled). This information may be useful for troubleshooting.

The information on this page is automatically refreshed at 15-second intervals. If CDP is disabled, a message appears at the top of the page and the list is empty. To enable CDP, see CDP Discovery, page 432.

Field	Description
Device ID	The host name of the neighboring device.
Local Port	The outgoing port that the security appliance is using for this connection.
Duration	The time interval (in seconds) that the security appliance will keep CDP information from a neighboring device.
Function	The neighbor's device type: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, or r - repeater.
Platform	The model number of the neighboring device.
Interface ID	The interface that the neighboring device is using for the connection.
IP Address	The IP address of the neighboring device.
Duplex	The duplex mode of the connection.
Voice VLAN	The Voice VLAN ID of the neighboring device.

Wireless Status (for ISA550W and ISA570W only)

Use the Wireless Status pages to view information about your wireless network. Refer to the following topics:

- **Wireless Status, page 99**
- **Client Status, page 100**

Wireless Status

Use the Wireless Status > Wireless Status page to view the cumulative total of relevant wireless statistics for all SSIDs. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

Wireless Status > Wireless Status

Field	Description
Wireless Status	
SSID Number	Number of the SSID.
SSID Name	Name of the SSID.
MAC Address	MAC address of the SSID.
VLAN	VLAN to which the SSID is mapped.
Client List	Number of client stations that are connected to the SSID.
Wireless Statistics	
Name	Name of the SSID.
Tx Packets	Number of transmitted packets on the SSID.
Rx Packets	Number of received packets on the SSID.
Collisions	Number of packet collisions reported to the SSID.
Tx Bytes/Sec	Number of transmitted bytes of information on the SSID.
Rx Bytes/Sec	Number of received bytes of information on the SSID.

Field	Description
Uptime	Time that the SSID has been active.

Client Status

Use the Wireless Status > Client Status page to view information for all client stations that are already connected to each SSID. The MAC address and IP address for all connected client stations for each SSID are displayed. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

NAT Status

Use the NAT Status page to view information for all NAT rules.

NAT Status

Field	Description
Original Source Address	Original source IP address in the packet.
Original Destination Address	Original destination IP address in the packet.
Source Port	Source interface that traffic comes from.
Destination Port	Destination interface that traffic goes to.
Translated Destination Address	IP address that the specified original destination address is translated to.
Translated Source Address	IP address that the specified original source address is translated to.
Translated Destination Port	Interface that the specified destination interface is translated to.
Translated Source Port	Interface that the specified source interface is translated to.

Field	Description
Tx Packets	Number of transmitted packets.
Rx Packets	Number of received packets.
Tx Bytes/Sec	Volume in bytes of transmitted traffic.
Rx Bytes/Sec	Volume in bytes of received traffic.

VPN Status

Use the VPN Status pages to view information for all VPN sessions. Refer to the following topics:

- IPsec VPN Status, page 101
- SSL VPN Status, page 103

IPsec VPN Status

Use the VPN Status > IPsec VPN Status page to view information for all IPsec VPN sessions. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

VPN Status > IPsec VPN Status

Field	Description
Active Sessions To manually terminate an active IPsec VPN session, click the **Disconnect** icon in the **Connect** column. To manually terminate multiple active IPsec VPN sessions, check them and click the **Disconnect** button. If an IPsec VPN session is terminated, you can manually establish the VPN connection by clicking the **Connect** icon in the **Connect** column.	
Name	VPN policy used for an IPsec VPN session.
Status	Connection status for an IPsec VPN session.

Field	Description
VPN Type	VPN connection type for an IPsec VPN session, such as Site-to-Site, IPsec Remote Access, or Teleworker VPN Client.
WAN Interface	WAN port used for an IPsec VPN session.
Remote Gateway	IP address of the remote peer. **NOTE:** For a site-to-site VPN session, it displays the IP address of the remote gateway. For an IPsec VPN session between the Teleworker VPN client and a remote IPsec VPN server, it displays the IP address of the IPsec VPN server. For an IPsec VPN session between the IPsec VPN server and a remote VPN client, it displays the IP address of the remote VPN client.
Local Network	Subnet IP address and netmask of your local network.
Remote Network	Subnet IP address and netmask of the remote network.
Statistics	
Name	VPN policy used for an IPsec VPN session.
VPN Type	VPN connection type for an IPsec VPN session.
WAN Interface	WAN port used for an IPsec VPN session.
Remote Gateway	IP address of the remote peer.
Local Network	Subnet IP address and netmask of your local network.
Remote Network	Subnet IP address and netmask of the remote network.
Tx Bytes	Volume of traffic in kilobytes transmitted from the VPN tunnel.
Rx Bytes	Volume of traffic in kilobytes received from the VPN tunnel.
Tx Packets	Number of IP packets transmitted from the VPN tunnel.
Rx Packets	Number of IP packets received from the VPN tunnel.

Field	Description
Teleworker VPN Client If the Teleworker VPN Client feature is enabled and the security appliance is acting as a Cisco VPN hardware client, the following information is displayed.	
Status	Shows if the Teleworker VPN Client feature is enabled or disabled.
Primary DNS	IP address of the primary DNS server.
Secondary DNS	IP address of the secondary DNS server.
Primary WINS	IP address of the primary WINS server.
Secondary WINS	IP address of the secondary WINS server.
Default Domain	Default domain name.
Split Tunnel	IP address and netmask for the specified split subnets.
Split DNS	IP address or domain name for the specified split DNS.
Backup Server 1/2/3	IP address or hostname for the specified backup servers.

SSL VPN Status

Use the VPN Status > SSL VPN Status page to view information for all active SSL VPN sessions. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

VPN Status > SSL VPN Status

Field	Description
Active Sessions To manually terminate an active SSL VPN session, click the **Disconnect** icon in the **Configure** column. To manually terminate multiple active SSL VPN sessions, check them and click the **Disconnect** button.	
Session ID	ID of the SSL VPN session.

Field	Description
User Name	Name of the connected SSL VPN user.
Client IP (Actual)	Actual IP address used by the SSL VPN client.
Client IP (VPN)	Virtual IP address of the SSL VPN client assigned by the SSL VPN gateway.
Connect Time	Amount of time since the SSL VPN user first established the connection.

SSL VPN Statistics

In the **Global Status** area, the global statistic information is displayed. To clear the global statistic information, click **Clear**.

Active Users	Total number of connected SSL VPN users.
In CSTP Frames	Number of CSTP frames received from all clients.
In CSTP Bytes	Total number of bytes in the CSTP frames received from all clients.
In CSTP Data	Number of CSTP data frames received from all clients.
In CSTP Control	Number of CSTP control frames received from all clients.
Out CSTP Frames	Number of CSTP frames sent to all clients.
Out CSTP Bytes	Total number of bytes in the CSTP frames sent to all clients.
Out CSTP Data	Number of CSTP data frames sent to all clients.
Out CSTP Control	Number of CSTP control frames sent to all clients.

In the **Session Statistics** table, the following information for each SSL VPN session is displayed.

To clear the statistic information for a single SSL VPN session, click **Clear** in the **Configure** column. To clear the statistic information for multiple SSL VPN sessions, check them and click **-Clear**.

Session ID	ID of the SSL VPN session.
In CSTP Frames	Number of CSTP frames received from the client.

Field	Description
In CSTP Bytes	Total number of bytes in the CSTP frames received from the client.
In CSTP Data	Number of CSTP data frames received from the client.
In CSTP Control	Number of CSTP control frames received from the client.
Out CSTP Frames	Number of CSTP frames sent to the client.
Out CSTP Bytes	Total number of bytes in the CSTP frames sent to the client.
Out CSTP Data	Number of CSTP data frames sent to the client.
Out CSTP Control	Number of CSTP control frames sent to the client.

NOTE CSTP is a Cisco proprietary protocol for SSL VPN tunneling. “In” represents that the packet comes from the client. “Out” represents that the packet is sent to the client. The client is the PC running the Cisco AnyConnect Secure Mobility Client software that connects to the security appliance running the SSL VPN server. A CSTP frame is a packet that carrying CSTP protocol information. There are two major frame types, control frames and data frames. Control frames implement control functions within the protocol. Data frames carry the client data, such as the tunneled payload.

Active User Sessions

Use the Active User Sessions page to view information for all active user sessions that are currently logged into the security appliance. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data. Click the **Logout** icon to terminate a web login user session or a VPN user session.

Active User Sessions

Field	Description
User Name	Name of the logged user.
IP Address	Host IP address from which the user accessed the security appliance.

Field	Description
Login Method	How the user logs into the security appliance, such as WEB, SSL VPN, IPsec Remote Access, or Captive Portal.
Session Time	Time that the user has logged into the security appliance.

Security Services Reports

Use the Security Services Reports pages to view the reports for all security services. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data. Refer to the following topics:

- **Web Security Report, page 106**
- **Anti-Virus Report, page 107**
- **Email Security Report, page 108**
- **Network Reputation Report, page 109**
- **IPS Report, page 110**
- **Application Control Report, page 111**

NOTE The security services reports are only active when the security license is validated. Before you choose a security service report to view, make sure that the corresponding security service is enabled.

Web Security Report

This report displays the number of web access requests logged and the number of websites blocked by Web URL Filtering, Web Reputation Filtering, or both.

STEP 1 In the **Web Security** tab, specify the following information:

- **Enable:** Check this box to enable the web security report, or uncheck this box to disable it.

- **Blocked Requests:** Check this box to display the number of websites blocked by Web URL Filtering and/or Web Reputation Filtering in the graph. To view more information about blocked requests, click the red bar in the graph. A pop-up window displays the following information for each blocked request: the date and the time, the IP address and the MAC address of the host that initiated the request, the web site, the blocked URL, the filter that blocked the request, and the number of times that the connection was blocked.
- **Processed Requests:** Check this box to display the number of web access requests logged by Web URL Filtering and/or Web Reputation Filtering in the graph.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of web access requests processed and total number of websites blocked since the Web URL Filtering and Web Reputation Filtering services were activated.
Total Last 7 Days	Total number of web access requests processed and total number of websites blocked in last seven days.
Total Today	Total number of web access requests processed and total number of websites blocked in one day.
Graph	Total number of web access requests processed and total number of websites blocked per day in last seven days.

Anti-Virus Report

This report displays the number of files checked and the number of viruses detected by the Anti-Virus service.

STEP 1 In the **Anti-Virus** tab, specify the following information:

- **Enable:** Check this box to enable the Anti-Virus report, or uncheck this box to disable it.

- **Detected Requests:** Check this box to display the number of viruses detected by the Anti-Virus service in the graph. To view more information about detected requests, click the red bar in the graph. A pop-up window displays the following information for each detected request: the date and the time, the IP address and the MAC address of the source and of the destination, the protocol used for the connection, the action taken, and the number of times a virus was found.
- **Processed Requests:** Check this box to display the number of files checked by the Anti-Virus service in the graph.

STEP 2 Click **Save** to save your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of files checked and total number of viruses detected since the Anti-Virus service was activated.
Total Last 7 Days	Total number of files checked and total number of viruses detected in last seven days.
Total Today	Total number of files checked and total number of viruses detected in one day.
Graph	Total number of files checked and total number of viruses detected per day in last seven days.

Email Security Report

This report displays the number of emails checked and the number of spam or suspected spam emails detected by the Spam Filter service.

STEP 1 In the **Email Security** tab, specify the following information:

- **Enable:** Check this box to enable the email security report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of spam or suspected spam emails detected by the Spam Filter service in the graph.

- **Processed Requests:** Check this box to display the number of emails checked by the Spam Filter service in the graph.

STEP 2 Click **Save** to save your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of emails checked and total number of spam or suspected spam emails detected since the Spam Filter service was activated.
Total Last 7 Days	Total number of emails checked and total number of spam or suspected spam emails detected in last seven days.
Total Today	Total number of emails checked and total number of spam or suspected spam emails detected in one day.
Graph	Total number of emails checked and total number of spam or suspected spam emails detected per day in last seven days.

Network Reputation Report

This report displays the number of packets checked and the number of packets blocked by the Network Reputation service.

STEP 1 In the **Network Reputation** tab, specify the following information:

- **Enable:** Check this box to enable the network reputation report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of packets blocked by the Network Reputation service in the graph.
- **Processed Requests:** Check this box to display the number of packets checked by the Network Reputation service in the graph.

STEP 2 Click **Save** to save your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of packets checked and total number of packets blocked since the Network Reputation service was activated.
Total Last 7 Days	Total number of packets checked and total number of packets blocked in last seven days.
Total Today	Total number of packets checked and total number of packets blocked in one day.
Graph	Total number of packets checked and total number of packets blocked per day in last seven days.

IPS Report

This report displays the number of packets detected and the number of packets dropped by the Intrusion Prevention (IPS) service.

STEP 1 In the **IPS** tab, specify the following information:

- **Enable:** Check this box to enable the IPS report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of packets dropped by the IPS service in the graph. To view more information about blocked requests, click the red bar in the graph. A pop-up window displays the following information for each blocked request: the date and time, the IP address and the MAC address of the source and of the destination, the action taken, and the number of times that this event was detected.
- **Processed Requests:** Check this box to display the number of packets detected by the IPS service in the graph.

STEP 2 Click **Save** to save your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of packets detected and total number of packets dropped since the IPS service was activated.
Total Last 7 Days	Total number of packets detected and total number of packets dropped in last seven days.
Total Today	Total number of packets detected and total number of packets dropped in one day.
Graph	Total number of packets detected and total number of packets dropped per day in last seven days.

Application Control Report

This report displays the number of packets detected and the number of packets blocked by the Application Control service.

STEP 1 In the **Application Control** tab, specify the following information:

- **Enable:** Check this box to enable the application control report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of packets dropped by the Application Control service in the graph. To view more information about blocked requests, click the red bar in the graph. A pop-up window displays the following information for each blocked request: the date and time, the IP address and the MAC address of the host that initiated the request, the blocked application, and the number of times that the application was blocked.
- **Processed Requests:** Check this box to display the number of packets detected by the Application Control service in the graph.

STEP 2 Click **Save** to save your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of packets detected and total number of packets blocked since the Application Control service was activated.
Total Last 7 Days	Total number of packets detected and total number of packets blocked in last seven days.
Total Today	Total number of packets detected and total number of packets blocked in one day.
Graph	Total number of packets detected and total number of packets blocked per day in last seven days.

System Status

Use the System Status pages to view information for all running processes and the system's CPU and memory utilization. Refer to the following topics:

- **Processes, page 112**
- **Resource Utilization, page 113**

Processes

Use the System Status > Processes page to view information for all running processes. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

System Status > Processes

Field	Description
Name	Name of the process that is running on your security appliance.
Description	Brief description for the running process.

Field	Description
Protocol	Protocol that is used by the socket.
Port	Port number of the local end of the socket.
Local Address	IP address of the local end of the socket.
Foreign Address	IP address of the remote end of the socket.

Resource Utilization

Use the System Status > Resource Utilization page to view information for the system's CPU and memory utilization.

System Status > Resource Utilization

Field	Description
CPU Utilization	
CPU Usage by User	CPU resource currently used by user space processes, in percentage.
CPU Usage by Kernel	CPU resource currently used by kernel space processes, in percentage.
CPU Idle	CPU idle resource at current time, in percentage.
CPU Waiting for I/O	CPU resource currently waiting for I/O, in percentage.
Memory Utilization	
Total Memory	Total amount of memory space available on the security appliance.
Memory Used	Total amount of memory space currently used by the processes.
Free Memory	Total amount of memory space currently not used by the processes.
Cached Memory	Total amount of memory space currently used as cache.

Field	Description
Buffer Memory	Total amount of memory space currently used as buffers.

4

Networking

Using the Networking module to configure your Internet connection, VLAN, DMZ, zones, routing, Quality of Service (QoS), and related features. It includes the following sections:

- Viewing Network Status, page 116
- Configuring IPv4 or IPv6 Routing, page 116
- Managing Ports, page 116
- Configuring the WAN, page 122
- Configuring a VLAN, page 137
- Configuring DMZ, page 141
- Configuring Zones, page 146
- Configuring DHCP Reserved IPs, page 149
- Configuring Routing, page 149
- Configuring Quality of Service, page 155
- Configuring IGMP, page 172
- Configuring VRRP, page 173
- Address Management, page 175
- Service Management, page 177

To access the Networking pages, click **Networking** in the left hand navigation pane.

Viewing Network Status

Use the Networking > Network Status pages to view the traffic statistics, the usage reports, the WAN bandwidth reports, all ARP (Address Resolution Protocol) entries, and DHCP address assignment. For descriptions of these status reports, see Network Status, page 88.

Configuring IPv4 or IPv6 Routing

Use the Networking > IPv4 or IPv6 Routing page to choose the IP routing mode for your network. Internet Protocol Version 6 (IPv6) is a new IP protocol designed to replace IPv4, the Internet protocol that is predominantly deployed and extensively used throughout the world. IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits, resulting in an exponentially larger address space. You can configure the security appliance to support IPv6 addressing on the WAN, LAN, and DMZ.

CAUTION In the current firmware, IPv6 functionalities are limited. ISA500 does not support firewall, VPN, and other security services for IPv6 in this firmware. We recommend enabling IPv6 for lab testing only with this firmware. Please check future firmware and release notes for information about any IPv6 updates.

STEP 1 Click **IPv4 or IPv6** to enable both IPv4 and IPv6 addressing, or click **IPv4 only** to enable only IPv4 addressing. By default, only IPv4 addressing is supported.

STEP 2 Click **Save** to save your settings.

Managing Ports

Use the Networking > Ports pages to configure the physical ports, port mirroring, and port-based access control settings. Refer to the following topics:

- **Viewing Status of Physical Interfaces, page 117**
- **Configuring Physical Ports, page 118**

- Configuring Port Mirroring, page 119
- Configuring Port-Based (802.1x) Access Control, page 120

Viewing Status of Physical Interfaces

Use the Networking > Ports > Physical Interface page to view information about all physical ports on the security appliance.

For all models, the following information appears:

- **Name:** The name of the physical port.
- **Enable:** Shows if the physical port is enabled or disabled.
- **Port Type:** The type of the physical port, such as WAN, LAN, or DMZ.
- **Mode:** The access mode of the physical port. A WAN or DMZ port is always set to the Access mode. A LAN port can be set to the Access or Trunk mode.
- **VLAN:** The VLANs to which the physical port is mapped.
- **PVID:** The Port VLAN ID (PVID) is used to forward or filter the untagged packets coming into port. The PVID of a trunk port is fixed to the DEFAULT VLAN (1).
- **Speed/Duplex:** The duplex mode (speed and duplex setting) of the physical port.
- **Link Status:** Shows if the physical port is connected or disconnected.

For the ISA550W and the ISA570W, the Wireless Interfaces area displays the following information for all SSIDs:

- **SSID Name:** The name of the SSID.
- **VLAN:** The VLAN to which the SSID is mapped.
- **Client Associated:** The number of client stations that are connected to the SSID.

  NOTE: To configure your wireless network, go to the Wireless pages. See Wireless (for ISA550W and ISA570W only), page 206.

STEP 1 Proceed as needed:

- Check the box in the **Enable** column to enable a physical port, or uncheck this box to disable the physical port.
- To edit the settings of a physical port, click the **Edit** (pencil) icon. See **Configuring Physical Ports, page 118**.

STEP 2 Click **Save** to apply your settings.

Configuring Physical Ports

After you click the Edit (pencil) icon on the Networking > Ports > Physical Interface page, use the Ethernet Configuration - Add/Edit page to enable or disable the selected physical port, assign it to one or more VLANs, and configure the duplex mode.

STEP 1 Enter the following information:

- **Name:** The name of the physical port.
- **Port Type:** The type of the physical port, such as WAN, LAN, or DMZ.
- **Mode:** Choose either **Access** or **Trunk** mode for a LAN port, or choose **Access** for a WAN or DMZ port. By default, all ports are set to the Access mode.
  - **Access:** All data going into and out of the Access port is untagged. Access mode is recommended if the port is connected to a single end-user device which is VLAN unaware.
  - **Trunk:** All data going into and out of the Trunk port is tagged. Untagged data coming into the port is not forwarded, except for the DEFAULT VLAN, which is untagged. Trunk mode is recommended if the port is connected to a VLAN-aware switch or router.
- **Port:** Click **On** to enable the port, or click **Off** to disable it. By default, all ports are enabled.
- **VLAN:** You can assign the physical port to VLANs.
  - To assign the port to a VLAN, choose an existing VLAN from the Available VLAN list and click the right arrows. The associated VLANs appear in the list of VLAN.

- To release the port from a VLAN, choose a VLAN from the VLAN list and click the left arrows.

NOTE: A LAN port can be assigned to multiple VLANs, but an Access LAN port can only be assigned to one VLAN. A DMZ port must be assigned to a DMZ network.

NOTE: You can click the **Create VLAN** link to create new VLANs. For information on configuring VLAN, see **Configuring a VLAN, page 137**.

- **Flow Control:** Click **On** to control the flow on the port, or click **Off** to disable it.

NOTE: Gigabit Ethernet flow control is provided by a PAUSE frame mechanism. A congested port sends an XON PAUSE frame, which causes the source port to stop sending data until an XOFF PAUSE frame is received. For this mechanism to work, flow control must be enabled on the source port and the destination port. Even with flow control enabled, the packet drops may occur if the receiving port runs out of buffers.

- **Speed:** Choose one of these options: AUTO, 10M, 100M, and 1000M. The default is AUTO for all ports. The AUTO option lets the system and network determine the optimal port speed.
- **Duplex:** Choose either Half or Full based on the port speed setting. The default is Full Duplex for all ports.
  - **Full:** The port supports transmissions between the device and the client in both directions simultaneously.
  - **Half:** The port supports transmissions between the device and the client in only one direction at a time.

STEP 2 Click **OK** to save your settings.

STEP 3 On the Networking > Ports > Physical Interface page, click **Save** to apply your settings.

Configuring Port Mirroring

Use the Networking > Ports > Port Mirroring page to allow traffic on one port to be visible on other ports. This feature is useful for debugging or traffic monitoring.

NOTE The dedicated WAN port (GE1) cannot be set as a destination or monitored port.

STEP 1 Click **On** to enable port mirroring, or click **Off** to disable this feature.

STEP 2 If you enable port mirroring, enter the following information:

- **TX Destination:** Choose the port that monitors the transmitted traffic for other ports.
- **TX Monitored Ports:** Check the ports that are monitored. The port that you set as a TX Destination port cannot be selected as a monitored port.
- **RX Destination:** Choose the port that monitors the received traffic for other ports.
- **RX Monitored Ports:** Check the ports that are monitored. The port that you set as a RX Destination port cannot be selected as a monitored port.

STEP 3 Click **Save** to apply your settings.

Configuring Port-Based (802.1x) Access Control

Use the Networking > Ports > Port-Based Access Control page to configure IEEE 802.1x port-based authentication, which prevents unauthorized devices (802.1x-capable clients) from gaining access to the network.

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a VLAN through publicly accessible ports. The authentication server authenticates each client (supplicant in Windows 2000, XP, Vista, Windows 7, and Mac OS) connected to a port before making available any service offered by the security appliance or the VLAN.

Until the client is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This feature simplifies the security management by allowing you to control access from a master database in a single server (although you can use up to three RADIUS servers to provide backups in case access to the primary server fails). It also means that user can enter the same authorized RADIUS username and password pair for authentication, regardless of which switch is the access point into the VLAN.

STEP 1 In the **RADIUS Settings** area, specify the RADIUS servers for authentication.

The security appliance predefines three RADIUS groups. Choose a predefined RADIUS group from the **RADIUS Index** drop-down list to authenticate users on 802.1x-capable clients. The RADIUS server settings of the selected group are displayed. You can edit the RADIUS server settings here but the settings that you specify will replace the default settings of the selected group. For information on configuring RADIUS servers, see Configuring RADIUS Servers, page 401.

STEP 2 In the **Port-Based Access Control Settings** area, perform the following actions:

- **Access Control:** Check this box to enable the 802.1x access control feature, or uncheck this box to disable it. This feature is not available for trunk ports.
- **Guest Authentication:** After you enable the 802.1x access control feature, check this box to enable the Guest Authentication feature, or uncheck this box to disable it.
- **Authorization Mode:** Specify the authorization mode for each physical port by clicking one of the following icons:
  - **Forced Authorized:** Disable the 802.1x access control feature and cause the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1x-based authentication of the client.
  - **Forced Unauthorized:** Cause the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The security appliance cannot provide authentication services to the client through the port.
  - **Auto:** Enable the 802.1x access control feature and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The security appliance requests the identity of the client and begins relaying authentication messages between the client and the authentication server. Each client attempting to access the network is uniquely identified by the security appliance by using the client's MAC address.

STEP 3 To specify the authenticated VLANs on a physical port, click the **Edit** (pencil) icon.

STEP 4 Enter the following information in the Port-Base Access Control - Edit page:

- **Access Control:** Check this box to enable the 802.1x access control feature.

- **Authenticated VLAN:** If you enable the 802.1x access control feature, choose the authenticated VLAN to which this port is assigned. The users who authenticated successfully can access the authenticated VLAN through the port. If the authentication fails, block access through the port.
- **Guest Authenticated:** If you enable the 802.1x access control feature, check this box to enable the Guest Authentication feature.
- **Authenticated VLAN:** If you enable the Guest Authentication feature, choose the guest VLAN to be associated with the port. If the authentication fails, the port is assigned to the selected guest VLAN instead of shutting down. For 802.1x-incapable clients, the port is also assigned to the selected guest VLAN when Guest Authentication is enabled.

STEP 5 Click **OK** to save your settings.

STEP 6 Click **Save** to apply your settings.

Configuring the WAN

By default, the security appliance is configured to receive a public IP address from your ISP automatically through DHCP. Depending on the requirements of your ISP, you may need to use the Networking > WAN pages modify the WAN settings to ensure Internet connectivity. Refer to the following topics:

- **Configuring WAN Settings for Your Internet Connection, page 122**
- **Configuring WAN Redundancy, page 130**
- **Configuring Link Failover Detection, page 132**
- **Configuring Dynamic DNS, page 134**

Configuring WAN Settings for Your Internet Connection

Use the Networking > WAN > WAN Settings to configure WAN settings by using the account information provided by your ISP. If you have two ISP links, you can configure one for WAN1 and another for WAN2.

Proceed as needed:

- **Release or renew a DHCP WAN connection, page 123**

- Configure the primary WAN, page 123
- Configure a secondary WAN, page 125

Release or renew a DHCP WAN connection

If a WAN interface is configured to obtain an IP address from the ISP by using Dynamic Host Configuration Protocol (DHCP), you can click the **Release** icon to release its IP address, or click the **Renew** icon to obtain a new IP address.

Configure the primary WAN

To configure the settings for the primary WAN (WAN1), click the **Edit** (pencil) icon. Then use the WAN - Add/Edit page to configure the connection. If you enabled IPv4/IPv6 routing mode, complete both tabbed pages. Click **OK** to save your settings. Click **Save** to apply your settings to the security appliance.

For IPv4 routing mode, enter the following information on the **IPv4** tab:

- **Physical Port:** The physical port associated with the primary WAN.
- **WAN Name:** The name of the primary WAN (WAN1).
- **IP Address Assignment:** Depending on the requirements of your ISP, choose the network addressing mode and complete the corresponding settings. The security appliance supports DHCP Client, Static IP, PPPoE, PPTP, and L2TP. For information on configuring network addressing mode, see Network Addressing Mode, page 125.
- **DNS Server Source:** DNS servers map Internet domain names to IP addresses. You can get DNS server addresses automatically from your ISP or use ISP-specified addresses.
  - **Get Dynamically from ISP:** Choose this option if you have not been assigned a static DNS IP address.
  - **Use these DNS Servers:** Choose this option if you have assigned a static DNS IP address. Also enter the addresses in the **DNS1** and **DNS2** fields.
- **MAC Address Source:** Specify the MAC address for the primary WAN. Typically, you can use the unique 48-bit local Ethernet address of the security appliance as your MAC address source.
  - **Use Default MAC Address:** Choose this option to use the default MAC address.

- **Use the following MAC address:** If your ISP requires MAC authentication and another MAC address has been previously registered with your ISP, choose this option and enter the MAC address that your ISP requires for this connection.

- **MAC Address:** Enter the MAC address, for example 01:23:45:67:89:ab.

- **Zone:** Choose the default WAN zone or an untrusted zone for the primary WAN. You can click the **Create Zone** link to view, edit, or add the zones on the security appliance.

For IPv4/IPv6 routing mode, enter the following information on the **IPv6** tab:

- **IP Address Assignment:** Choose **Static IP** if your ISP assigned a fixed (static or permanent) IP address, or choose **SLAAC** if you were not assigned a static IP address. By default, your security appliance is configured to be a DHCPv6 client of the ISP, with stateless address auto-configuration (SLAAC).

  - **SLAAC:** SLAAC provides a convenient method to assign IP addresses to IPv6 nodes. This method does not require any human intervention from an IPv6 user. If you choose SLAAC, the security appliance can generate its own addresses using a combination of locally available information and information advertised by routers.

  - **Static IP:** If your ISP assigned a static IPv6 address, configure the IPv6 WAN connection in the following fields:

    IPv6 Address: Enter the static IP address that was provided by your ISP.

    IPv6 Prefix Length: The IPv6 network (subnet) is identified by the initial bits of the address called the prefix. All hosts in the network have the identical initial bits for their IPv6 address. Enter the number of common initial bits in the network's addresses. The default prefix length is 64.

    Default IPv6 Gateway: Enter the IPv6 address of the gateway for your ISP. This is usually provided by the ISP or your network administrator.

    Primary DNS Server: Enter a valid IP address of the primary DNS server.

    Secondary DNS Server (Optional): Optionally, enter a valid IP address of the secondary DNS server.

Configure a secondary WAN

To configure a secondary WAN (WAN2), click **Add**. Then use the WAN - Add/Edit page to configure the connection. If you enabled IPv4/IPv6 routing mode, complete both tabbed pages, as described for the primary WAN interface. Click **OK** to save your settings in the pop-up window. Click **Save** to apply your settings to the security appliance. To determine how the two ISP links are used, configure the WAN redundancy settings. See **Configuring WAN Redundancy, page 130**.

- If you are having problems with your WAN connection, see Internet Connection, page 453.

Network Addressing Mode

The security appliance supports five types of network addressing modes. You need to specify the network addressing mode for the primary WAN and the secondary WAN depending on your ISP requirements.

NOTE Confirm that you have proper network information from your ISP or a peer router to configure the security appliance to access the Internet.

Network Addressing Mode	Configuration
DHCP Client	Connection type often used with cable modems. Choose this option if your ISP dynamically assigns an IP address on connection. **NOTE:** Unless a change is required by your ISP, it is recommended that the MTU values be left as is. ▪ **MTU:** The Maximum Transmission Unit is the size, in bytes, of the largest packet that can be passed on. Choose **Auto** to use the default MTU size, or choose **Manual** if you want to specify another size. ▪ **MTU Value:** If you choose **Manual**, enter the custom MTU size in bytes.

Network Addressing Mode	Configuration
Static IP	Choose this option if the ISP provides you with a static (permanent) IP address and does not assign it dynamically. Use the corresponding information from your ISP to complete the following fields: ▪ **IP Address:** Enter the IP address of the WAN port that can be accessible from the Internet. ▪ **Subnet Mask:** Enter the IP address of the subnet mask. ▪ **Gateway:** Enter the IP address of default gateway. ▪ **MTU:** The Maximum Transmission Unit is the size, in bytes, of the largest packet that can be passed on. Choose **Auto** to use the default MTU size, or choose **Manual** if you want to specify another size. ▪ **MTU Value:** If you choose **Manual**, enter the custom MTU size in bytes.

Network Addressing Mode	Configuration
PPPoE	PPPoE uses Point to Point Protocol over Ethernet (PPPoE) to connect to the Internet. Choose this option if your ISP provides you with client software, username, and password. Use the necessary PPPoE information from your ISP to complete the PPPoE configuration. ▪ **User Name:** Enter the username that is required to log into the ISP. ▪ **Password:** Enter the password that is required to log into the ISP. ▪ **Authentication Type:** Choose the authentication type specified by your ISP. ▪ **Connect Idle Time:** Choose this option to let the security appliance disconnect from the Internet after a specified period of inactivity (Idle Time). This choice is recommended if your ISP fees are based on the time that you spend online. ▪ **Keep alive:** Choose this option to keep the connection always on, regardless of the level of activity. This choice is recommended if you pay a flat fee for your Internet service. ▪ **MTU:** Choose **Auto** to use the default MTU size, or choose **Manual** if you want to specify another size. ▪ **MTU Value:** If you choose **Manual**, enter the custom MTU size in bytes. ▪ **Add VLAN Tag:** Click **Yes** to support VLAN Tagging (802.1q) over the WAN port, or click **No** to disable it. ▪ **VLAN Tag ID:** Specify the VLAN tag (ID) to the WAN port. ▪ **Reset Timer:** You can reset the PPPoE connection at a given time of a day and day of a week. The reset events are logged if you enable this feature. Choose one of the following options from the **Frequency** drop-down list and specify the corresponding settings: - **Never:** Choose this option to disable this feature. - **Daily:** Choose this option to reset the PPPoE connection at a given time of a day. Specify the time of a day in the **Time** fields. - **Weekly:** Choose this option to reset the PPPoE connection at a given day of a week. Then specify the day of a week and the time of a day.

Network Addressing Mode	Configuration
PPTP	The PPTP protocol is typically used for VPN connection. Use the necessary information from your ISP to complete the PPTP configuration: ▪ **IP Address:** Enter the IP address of the WAN port that can be accessible from the Internet. ▪ **Subnet Mask:** Enter the subnet mask. ▪ **Gateway:** Enter the IP address of default gateway. ▪ **User Name:** Enter the username that is required to log into the PPTP server. ▪ **Password:** Enter the password that is required to log into the PPTP server. ▪ **PPTP Server IP Address:** Enter the IP address of the PPTP server. ▪ **MPPE Encryption:** Microsoft Point-to-Point Encryption (MPPE) encrypts data in PPP-based dial-up connections or PPTP VPN connections. Check this box to enable the MPPE encryption to provide data security for the PPTP connection that is between the VPN client and the VPN server. ▪ **Connect Idle Time:** Choose this option to let the security appliance disconnect from the Internet after a specified period of inactivity (Idle Time). This choice is recommended if your ISP fees are based on the time that you spend online. ▪ **Keep alive:** Choose this option to keep the connection always on, regardless of the level of activity. This choice is recommended if you pay a flat fee for your Internet service. ▪ **MTU:** Choose **Auto** to use the default MTU size, or choose **Manual** if you want to specify another size. ▪ **MTU Value:** If you choose **Manual**, enter the custom MTU size in bytes.

Network Addressing Mode	Configuration
L2TP	Choose this option if you want to use IPsec to connect a L2TP (Layer 2 Tunneling Protocol) server and encrypt all data transmitted from the client to the server. However, it does not encrypt network traffic to other destinations. Use the necessary information from your ISP to complete the L2TP configuration: ▪ **IP Address:** Enter the IP address of the WAN port that can be accessible from the Internet. ▪ **Subnet Mask:** Enter the subnet mask. ▪ **Gateway:** Enter the IP address of default gateway. ▪ **User Name:** Enter the username that is required to log into the L2TP server. ▪ **Password:** Enter the password that is required to log into the L2TP server. ▪ **L2TP Server IP Address:** Enter the IP address of the L2TP server. ▪ **Secret (Optional):** L2TP incorporates a simple, optional, CHAP-like tunnel authentication system during control connection establishment. Enter the secret for tunnel authentication if necessary. ▪ **Connect Idle Time:** Choose this option to let the security appliance disconnect from the Internet after a specified period of inactivity (Idle Time). This choice is recommended if your ISP fees are based on the time that you spend online. ▪ **Keep alive:** Choose this option to keep the connection always on, regardless of the level of activity. This choice is recommended if you pay a flat fee for your Internet service. ▪ **MTU:** Choose **Auto** to use the default MTU size, or choose **Manual** if you want to specify another size. ▪ **MTU Value:** If you choose **Manual**, enter the custom MTU size in bytes.

Configuring WAN Redundancy

If you have two ISP links, one for WAN1 and another for WAN2, use the Networking > WAN Redundancy pages to configure the WAN redundancy to determine how the two ISP links are used. Refer to the following topics:

- **Dual WAN Settings, page 130**
- **Load Balancing with Policy-Based Routing Configuration Example, page 133**

NOTE Before you configure the WAN redundancy settings, you must first configure the secondary WAN connection. See **Configure a secondary WAN, page 125**.

NOTE When the security appliance is working in the Dual WAN Settings or Failover mode, if one WAN link is down such as the cable is disconnected, the WAN redundancy and Policy-Based Routing settings are ignored and all traffic is handled by the active WAN port.

Dual WAN Settings

Use the Networking > WAN Redundancy > Dual WAN Settings page to segregate traffic between links that are not of the same speed. For example, you can bind the high-volume services through the port that is connected to a high speed link, and bind the low-volume services to the port that is connected to the slower link.

Load balancing is implemented for outgoing traffic and not for incoming traffic. To maintain better control of WAN port traffic, consider making the WAN port Internet address public and keeping the other one private.

NOTE To configure load balancing, make sure that you configure both WAN ports to keep alive. If the WAN port is configured to time out after a specified period of inactivity, then load balancing is not applicable.

STEP 1 Choose an option in the Dual WAN Settings section to specify how the two ISP links are used. The two links will carry data for the protocols that are bound to them.

- **Weighted Dual WAN Settings:** Distributes the bandwidth to two WAN ports by the weighted percentage or by the weighted link bandwidth. If you choose this mode, choose one of the following options and finish the settings:
  - **Weighted by Percentage:** If you choose this option, specify the percentage for each WAN, such as 80% bandwidth for WAN1 and at least 20% bandwidth for WAN2.

- **Weighted by Link Bandwidth:** If you choose this option, specify the amount of bandwidth for each WAN, such as 80 Mbps for WAN1 and 20 Mbps for WAN2, which indicates that 80% bandwidth is distributed to WAN1 and at least 20% bandwidth is distributed to WAN2.

NOTE: The Weighted by Link Bandwidth option has the same effect with the Weighted by Percentage option. It just provides more percentage options than Weighted by Percentage that only provides three percentage options. For example, you can set 60 Mbps for WAN1 and 40 Mbps for WAN2, which indicates that 60% bandwidth is distributed to WAN1 and the remaining 40% bandwidth is distributed to WAN2.

- **Based on Real-time Bandwidth:** Sends traffic to the link that has the highest real-time bandwidth. Use information from your service provider to specify the base bandwidth for each link in the **WAN1** and **WAN2** fields.
- **Failover:** If a failure is detected on the primary link, then the security appliance diverts all Internet traffic to the backup link. When the primary link regains connectivity, all Internet traffic is directed to the primary link and the backup link becomes idle. By default, WAN1 is set as the primary link and the WAN2 is set as the backup link.

  NOTE: When the security appliance is working in the Failover mode, the Policy-Based Routing settings will be ignored.

  - **Select WAN Precedence:** Choose which link to use as the primary link and the secondary link. The default option is Primary: WAN1; Secondary: WAN2.
  - **Preempt Delay Timer:** Enter the time in seconds that the security appliance will wait before sending traffic to the primary link from the backup link after the primary link is up again. The default value is 5 seconds.
- **Routing Table:** Uses the static routing policies to determine the types of traffic that pass through the two WAN links. For information on configuring static routing, see **Configuring Static Routing, page 151**.

STEP 2 Enable **Policy Based Routing** if you want to use policies to specify the internal IP and/or service going through each WAN port to provide more flexible and granular traffic handling capabilities. Click **On** to enable this feature, or click **Off** to disable it. After enabling this feature, click **Configure** to set the policies. See **Configuring Policy-Based Routing, page 153**.

NOTE: If you enable Policy-Based Routing, the policy-based routing settings will take precedence over the load balancing settings. Traffic matching the policy-based routing policies will be routed based on these settings. Traffic not matching the policy-based routing policies will be routed based on the load balancing settings.

STEP 3 Click **Save** to apply your settings.

Configuring Link Failover Detection

Use the Networking > WAN > WAN Redundancy > Link Failover Detection page to detect the link failure. If a failure occurs, traffic for the unavailable link is diverted to the active link.

STEP 1 Enter the following information:

- **Failover Detection:** Click **On** to enable the Link Failover Detection feature, or click **Off** to disable it.
- **Retry Count:** Enter the number of retries. The security appliance repeatedly tries to connect to the ISP after the link failure is detected. The default value is 5.
- **Retry Timeout:** If the connection to the ISP is down, the security appliance tries to connect to the ISP after a specified timeout. Enter the timeout, in seconds, to re-connect to the ISP. The default value is 5 seconds.
- **Ping Detection:** Choose this option to detect the WAN failure by pinging the IP address that you specify in the following fields:
  - **Default IP Gateways:** Ping the IP address of default WAN gateway. If the default WAN gateway can be detected, the network connection is active.
  - **Specify the IP Gateways:** Ping the specified remote hosts. Enter the IP addresses in the **Primary IP Gateway** and **Secondary IP Gateway** fields. In Failover mode, if the primary WAN remote host can be detected, the network connection is active. When using Dual WAN Settings, if the remote hosts for both WAN ports can be detected, the WAN connection is active.

- **DNS Detection:** Choose this option to detect the WAN failure by looking up the DNS servers that you specify in the following fields:
  - **Default DNS Servers:** Send the DNS query for www.cisco.com to the default WAN DNS server. If the DNS server can be detected, the network connection is active.
  - **Specify DNS Servers:** Send the DNS query for www.cisco.com to the specified DNS servers. Enter the IP addresses in the **Primary WAN DNS Server** and **Secondary WAN DNS Server** fields. If the primary or secondary DNS server can be detected, the network connection is active.

STEP 2 Click **Save** to apply your settings.

Load Balancing with Policy-Based Routing Configuration Example

Use Case: A customer has two lines, one is a cable link and another is a DSL link. The majority of traffic goes through the cable link since it has larger bandwidth, and the rest traffic goes through the DSL link. As lots of secure websites (such as bank, or online shopping) are sensitive to flip flop the source IP address, let traffic for https, ftp, video, and game go through the cable link.

Solution: Complete the following configuration tasks:

- Configure a configurable port as the secondary WAN (WAN2). See **Configure a secondary WAN, page 125**.
- Connect the cable modem to the primary WAN port (WAN1) and connect the DSL modem to the secondary WAN port (WAN2).
- Enable the Weighted Dual WAN Settings and set the weighted value of WAN1 to 80% and the weighted value of WAN2 to 20%. See **Dual WAN Settings, page 130**.
- Enable the Policy-Based Routing feature and configure the Policy-Based Routing rules so that traffic for HTTPS, FTP, video, and game is directed to WAN1. See **Configuring Policy-Based Routing, page 153**.
- (Optional) Enable the Usage reports and the WAN Bandwidth reports so that you can view the network bandwidth usage. See **Usage Reports, page 92** and WAN Bandwidth Reports, page 94.

Configuring Dynamic DNS

Use the Networking > WAN > DDNS page to configure Dynamic DNS (DDNS). DDNS is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. If your ISP has not provided you with a static IP and your WAN connection is configured to use DHCP to obtain an IP address dynamically, then DDNS provides the domain name to map the dynamic IP address for your website. To use DDNS, you must set up an account with a DDNS provider such as DynDNS.com.

DDNS Services Table

The **Status** column displays the status of DDNS service. Click **Active** to manually update the IP address of the WAN interface to the user-specified domain name.

- **Non-active:** The DDNS service is not active (DDNS daemon does not start).
- **Active (initial):** The DDNS daemon starts but the DDNS updating process is not complete yet.
- **Active (updated WAN**x**):** The DDNS updating process is complete and the address of the WAN interface is updated to the user-specified domain name.

Adding or modifying a DDNS service

Click **Add** to add a new DDNS service. To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon.

STEP 1 Enter the following information:

- **Service:** Specify the provider for your DDNS service. You can choose either DynDNS or No-IP service.

  NOTE: You must sign up for an account with either one of these providers before you can use this service.

- **Active on Startup:** Check this box to activate the DDNS service when the security appliance starts up.
- **WAN Interface:** Choose the WAN port for the DDNS service. Traffic for the DDNS services will pass through the specified WAN port.

  NOTE: If the WAN redundancy is set as the Failover mode, this option is grayed out. When WAN failover occurs, DDNS will switch traffic to the active WAN port.

- **User Name:** Enter the username of the account that you registered in the DDNS provider.

- **Password:** Enter the password of the account that you registered in the DDNS provider.
- **Host and Domain Name:** Enter the complete host name and domain name for the DDNS service, for example: name.dyndns.org.
- **Wildcards:** Check this box to allow all subdomains of your DDNS host name to share the same public IP address as the host name.
- **Update:** Check this box to update the host information every week.

STEP 2 Click **OK** to save your settings and close the pop-up window.

STEP 3 Click **Save** to apply your settings.

Measuring and Limiting Traffic with the Traffic Meter

Use the Networking > WAN > Traffic Metering pages to measure and limit traffic routed by the security appliance. If you enabled a secondary WAN link, use the navigation tree to choose either Primary WAN Metering or Secondary WAN Metering.

STEP 1 In the **Traffic Meter** area, enter the following information:

- **Enable:** Click **On** to enable traffic metering on the port, or click **Off** to disable it. Enabling this feature on the port will keep a record of the volume of traffic going from this port.
- **Traffic Limit:** Specify the restriction on the volume of data being transferred through the port.
  - **No Limit:** The default option, where no limits on data transfer are imposed.
  - **Download Only:** Limit the amount of download traffic. Enter the maximum allowed data in Megabytes that can be downloaded for a given month in the **Monthly Limit** field. After the limit is reached, no traffic is allowed from the WAN side.
  - **Both Directions:** Calculate traffic for both upload and download directions. The traffic limit entered into the **Monthly Limit** field is shared by both upload and download traffic. For example, for a 1 GB limit, if a 700 MB file is downloaded then the remaining 300 MB must be shared

between both upload and download traffic. The amount of traffic downloaded will reduce the amount of traffic that can be uploaded and vice-versa.

- **Monthly Limit:** Enter the volume limit that is applicable for this month. This limit will apply to the type of direction (Download Only or Both Direction) selected above. The value of zero (0) indicates that all traffic through this port will be blocked.

STEP 2 In the **Traffic Counter** area, enter the following information:

- **Traffic Counter:** Specify the action to be taken on the traffic counter.
  - **Restart Now:** Choose this option and then click **Save** to reset the counter immediately.
  - **Specific Time:** Choose this option if you want the counter to restart at a specified day and time. Then enter the time in hours (hh) and minutes (mm) and select the day of the month in the **Reset Time** area.
- **Send Email Report:** Click **On** to send an alert email to the specified email address before the traffic counter is reset, or click **Off** to disable it. This feature requires that you enable the Traffic Meter Alert feature and configure the email server settings on the Email Alert Settings page. See Configuring Email Alert Settings, page 408.

STEP 3 In the **When Limit is Reached** area, specify the action when the traffic limit is reached.

- **Traffic Block:** Choose one of the following options:
  - **All Traffic:** Block all traffic through the WAN port when the traffic limit is reached.
  - **All Traffic Except Email:** Block all traffic except email through the WAN port when the traffic limit is reached.
- **Email Alert:** Click **On** to send an alert email to the specified email address when the traffic limit is reached, or click **Off** to disable it. This feature requires that you enable the Traffic Meter Alert feature and configure the email server settings on the Email Alert Settings page. See Configuring Email Alert Settings, page 408.

STEP 4 In the **Internet Traffic** area, the following information is displayed after you enable Traffic Metering:

Start Date/Time	Date on which the traffic meter was started or the last time that the traffic counter was reset.
Outgoing Traffic Volume	Volume of traffic, in Megabytes, that was uploaded through this port.
Incoming Traffic Volume	Volume of traffic, in Megabytes, that was downloaded through this port.
Average per day	Average volume of traffic that passed through this port.
Traffic Utilized	Amount of traffic, in percent, that passed through this port against the monthly limit.

STEP 5 Click **Save** to apply your settings.

Configuring a VLAN

Use the Networking > WAN > VLAN page to configure a Virtual LAN (VLAN). VLANs allow you to segregate and isolate traffic. A PC on one VLAN cannot access the network resources on other VLANs.

The security appliance predefines three VLANs:

- A native VLAN (DEFAULT), with VLAN ID 1 and IP address 192.168.75.1. By default, this VLAN is in the LAN zone.
- A guest VLAN (GUEST), with VLAN ID 2 and IP address 192.168.25.1. By default, this VLAN is in the GUEST zone.
- A voice VLAN (VOICE) with VLAN ID 100 and IP address 10.1.1.2. By default, this VLAN is in the VOICE zone.

You can change the settings for predefined VLANs or add new VLANs to meet your business needs.

NOTE Up to 16 VLANs can be configured on the security appliance.

STEP 1 To add a new VLAN, click **Add**. To modify the settings for a VLAN, click the **Edit** (pencil) icon.

Other options: To delete a VLAN, click the **Delete** (x) icon. The default VLANs cannot be deleted.

STEP 2 In the **Basic Settings** tab, enter the following information:

- **Name:** Enter the name for the VLAN.
- **VLAN ID:** Enter a unique identification number for the VLAN, which can be any number from 3 to 4089. The VLAN ID 1 is reserved for the DEFAULT VLAN and the VLAN ID 2 is reserved for the GUEST VLAN.
- **IP Address:** Enter the subnet IP address for the VLAN.
- **Netmask:** Enter the subnet mask for the VLAN.
- **Spanning Tree:** Check this box to enable the Spanning Tree feature to determine if there are loops in the network topology. The Spanning Tree Protocol (STP) is a link layer network protocol that ensures a loop-free topology for any bridged LAN. The STP is used to prevent bridge loops and to ensure broadcast radiation.
- **Voice VLAN:** Check the box if you want voice applications to use this VLAN.
- **Port:** Assign the LAN ports to the VLAN. Traffic through the selected LAN ports is directed to the VLAN. All available ports including the dedicated LAN ports and the configurable ports appear in the **Port** list.

  Choose the ports from the **Port** list and click **Access** to add them to the **Member** list and set the selected ports as the Access mode. Alternatively, you can choose the ports from the **Port** list and click **Trunk** to add them to the **Member** list and set the selected ports as the Trunk mode.

  NOTE: This setting will change the port type and access mode of the selected physical ports. For example, choose a port that was set as a DMZ port and add it to the Member list. The DMZ port will be configured as a LAN port. Changing the port type will wipe out all configuration relative to the physical port.
- **Zone:** Choose the zone to which the VLAN is mapped. By default, the DEFAULT VLAN is mapped to the LAN zone, the GUEST VLAN is mapped to the GUEST zone, and the VOICE VLAN is mapped to the VOICE zone. You can click the **Create Zone** link to view, edit, or add the zones on the security appliance.

STEP 3 In the **DHCP Pool Settings** tab, choose the DHCP mode from the **DHCP Mode** drop-down list.

- **Disable:** Choose this option if the computers on the VLAN are configured with static IP addresses or are configured to use another DHCP server.
- **DHCP Server:** Allows the security appliance to act as a DHCP server and assigns IP addresses to all devices that are connected to the VLAN. Any new DHCP client joining the VLAN is assigned an IP address of the DHCP pool.
- **DHCP Relay:** Allows the security appliance to use a DHCP Relay. If you choose DHCP Relay, enter the IP address of the remote DHCP server in the **Relay IP** field.

STEP 4 If you choose **DHCP Server** as the DHCP mode, enter the following information:

- **Start IP:** Enter the starting IP address of the DHCP pool.
- **End IP:** Enter the ending IP address of the DHCP pool.

  NOTE: The Start IP address and End IP address should be in the same subnet with the VLAN IP address.
- **Lease Time:** Enter the maximum connection time that a dynamic IP address is “leased” to a network user. When the time elapses, the user will be automatically renewed the dynamic IP address.
- **DNS1:** Enter the IP address of the primary DNS server.
- **DNS2:** Optionally, enter the IP address of the secondary DNS server.
- **WINS1:** Optionally, enter the IP address of the primary WINS server.
- **WINS2:** Optionally, enter the IP address of the secondary WINS server.
- **Domain Name:** Optionally, enter the domain name for the VLAN.
- **Default Gateway:** Enter the IP address for default gateway.
- **Option 66:** Provides provisioning server address information to hosts requesting this option. Only supports the IP address or host name of a single TFTP server. Enter the IP address of the single TFTP server for the VLAN.
- **Option 67:** Provides a configuration/bootstrap file name to the hosts requesting this option. This is used in conjunction with the option 66 to allow the client to form an appropriate TFTP request for the file. Enter the configuration/bootstrap file name on the specified TFTP server.

- **Option 150:** Supports a list of TFTP servers (2 TFTP servers). Enter the IP addresses of TFTP servers. Separate multiple entries with commas (,).

  NOTE: Enterprises with small branch offices that implement a Cisco IP Telephony Voice over IP solution typically implement Cisco CallManager at a central office to control Cisco IP Phones at small branch offices. This implementation allows centralized call processing, reduces the equipment required, and eliminates the administration of additional Cisco CallManager and other servers at branch offices. Cisco IP Phones download their configuration from a TFTP server. When a Cisco IP Phone starts, if it does not have both the IP address and TFTP server IP address pre-configured, it sends a request with option 150 or 66 to the DHCP server to obtain this information.

STEP 5 In the **IPv6 Setting** tab, specify IPv6 addressing for the VLAN if you enable the IIPv4 or Pv6 mode.

- **IPv6 Address:** Enter the IPv6 address based on your network requirements.
- **IPv6 Prefix Length:** Enter the number of characters in the IPv6 prefix.

  The IPv6 network (subnet) is identified by the prefix, which consists of the initial bits of the address. The default prefix length is 64 bits. All hosts in the network have the identical initial bits for the IPv6 address. The number of common initial bits in the addresses is set by the prefix length field.

STEP 6 Click **OK** to save your settings and close the pop-up window.

STEP 7 Click **Save** to apply your settings.

STEP 8 If you want to reserve certain IP addresses for specified devices, go to the Networking > DHCP Reservations page. See **Configuring DHCP Reserved IPs, page 149**. You must enable the DHCP Server or DHCP Relay mode for this purpose.

Configuring DMZ

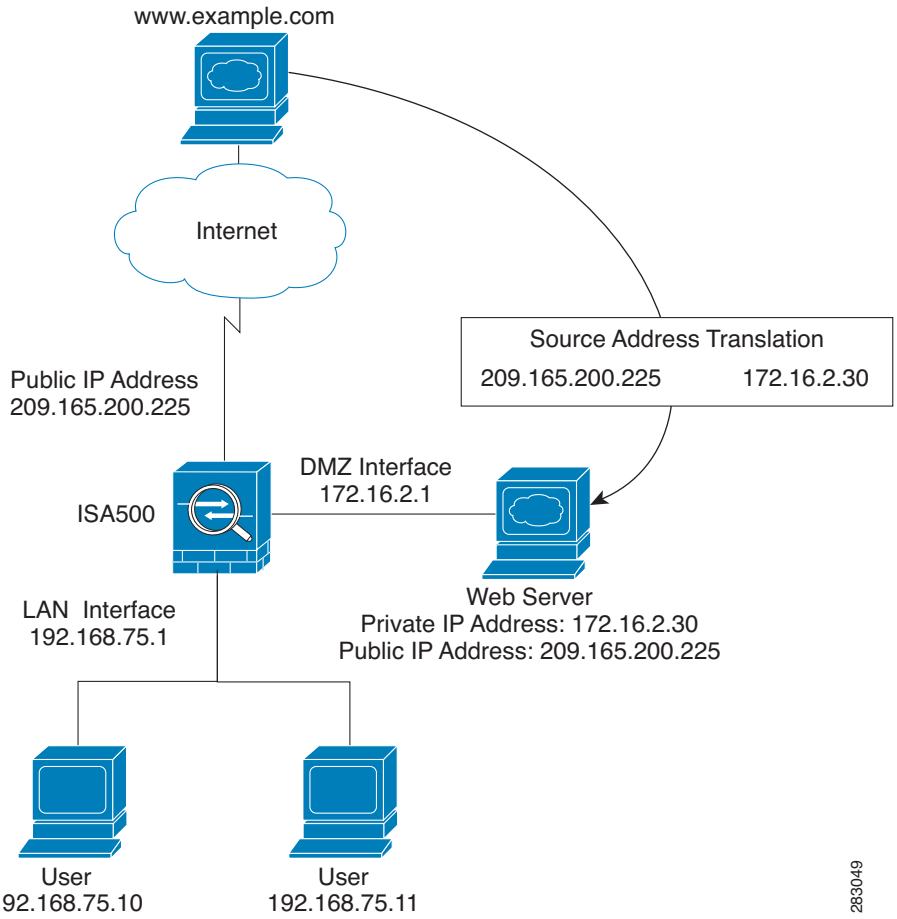
Use the Networking > DMZ page to configure a Demarcation Zone or Demilitarized Zone (DMZ). A DMZ is a sub-network that is behind the firewall but that is open to the public. By placing your public services on a DMZ, you can add an additional layer of security to the LAN. The public can connect to the services on the DMZ but cannot penetrate the LAN. You should configure your DMZ to include any hosts that must be exposed to the WAN (such as web or email servers).

About DMZ networks

This section describes how to configure the DMZ networks. The DMZ configuration is identical to the VLAN configuration. There are no restrictions on the IP address or subnet assigned to the DMZ port, except it cannot be identical to the IP address given to the predefined VLANs.

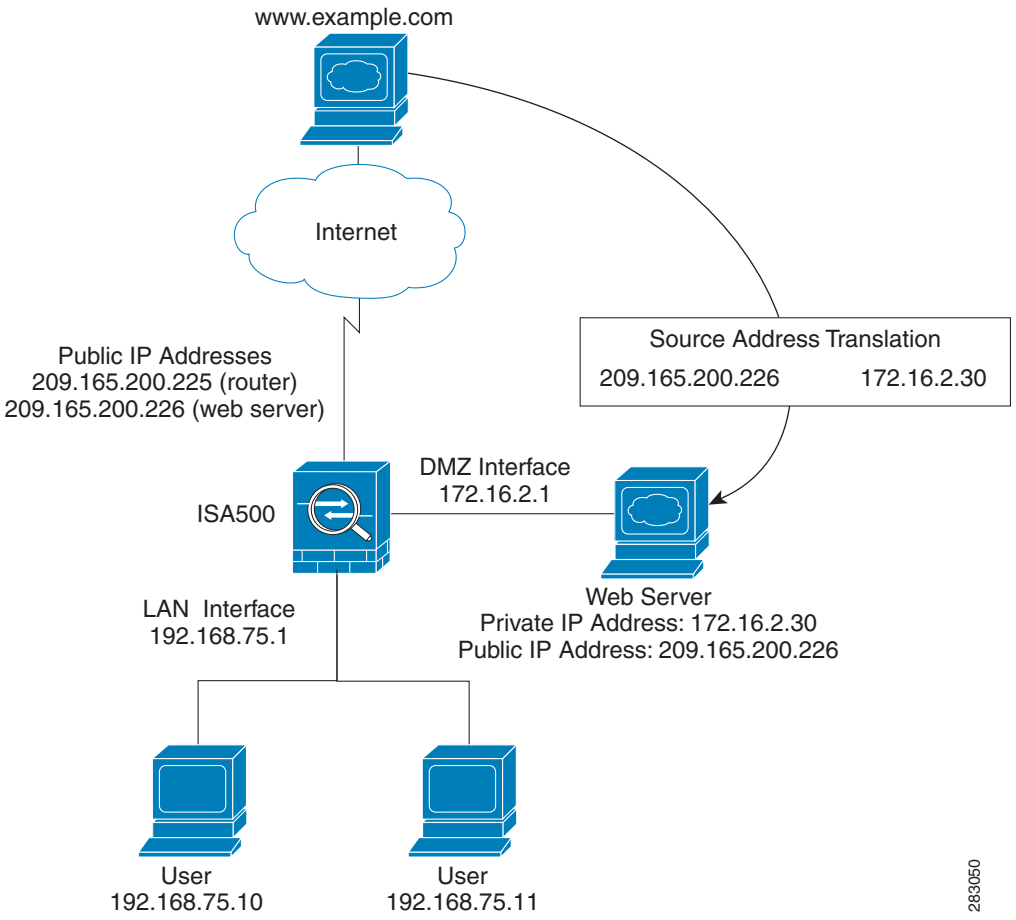
NOTE Up to 4 DMZs can be configured on the security appliance.

Figure 1 Example DMZ with One Public IP Address for WAN and DMZ



In this scenario, the business has one public IP address, 209.165.200.225, which is used for both the security appliance's public IP address and the web server's public IP address. The administrator configures the configurable port to be used as a DMZ port. A firewall rule allows inbound HTTP traffic to the web server at 172.16.2.30. Internet users enter the domain name that is associated with the IP address 209.165.200.225 and can then connect to the web server. The same IP address is used for the WAN interface.

Figure 2 Example DMZ with Two Public IP Addresses



In this scenario, the ISP has supplied two static IP addresses: 209.165.200.225 and 209.165.200.226. The address 209.165.200.225 is used for the security appliance's public IP address. The administrator configures the configurable port to be used as a DMZ port and created a firewall rule to allow inbound HTTP traffic to the web server at 172.16.2.30. The firewall rule specifies an external IP address of 209.165.200.226. Internet users enter the domain name that is associated with the IP address 209.165.200.226 and can then connect to the web server.

Configuring a DMZ

STEP 1 To add a new DMZ, click **Add**. To modify the settings for a DMZ, click the **Edit** (pencil) icon.

Other options: To delete a DMZ, click the **Delete** (x) icon.

STEP 2 In the **Basic Settings** tab, enter the following information:

- **Name:** Enter the name for the DMZ.
- **IP Address:** Enter the subnet IP address for the DMZ.
- **Netmask:** Enter the subnet mask for the DMZ.
- **Spanning Tree:** Check this box to enable the Spanning Tree feature to determine if there are loops in the network topology.
- **Port:** Specify a configurable port as a DMZ port. Traffic through the DMZ port is directed to the DMZ. All available configurable ports appear in the **Port** list. Choose a port from the **Port** list and add it to the **Member** list. The selected configurable port will be set as a DMZ port.

  NOTE: This setting will change the port type and access mode of the selected configurable port. Changing the port type will wipe out all configuration relative to the physical port.
- **Zone:** Choose the default DMZ zone or a custom DMZ zone to which the DMZ is mapped. You can click the **Create Zone** link to view, edit, or add the zones on the security appliance.

STEP 3 In the **DHCP Pool Settings** tab, choose the DHCP mode from the **DHCP Mode** drop-down list.

- **Disable:** Choose this option if the computers on the DMZ are configured with static IP addresses or are configured to use another DHCP server.
- **DHCP Server:** Allows the security appliance to act as a DHCP server and assigns IP addresses to all devices that are connected to the DMZ. Any new DHCP client joining the DMZ is assigned an IP address of the DHCP pool.
- **DHCP Relay:** Allows the security appliance to use a DHCP Relay. If you choose DHCP Relay, enter the IP address of the remote DHCP server in the **Relay IP** field.

STEP 4 If you choose **DHCP Server** as the DHCP mode, enter the following information:

- **Start IP:** Enter the starting IP address in the DHCP range.
- **End IP:** Enter the ending IP address in the DHCP range.

  NOTE: The Start and End IP addresses must be in the same subnet with the DMZ IP address.

- **Lease Time:** Enter the maximum connection time that a dynamic IP address is “leased” to a network user. When the time elapses, the user will be automatically renewed the dynamic IP address.
- **DNS 1:** Enter the IP address of the primary DNS server.
- **DNS 2:** Optionally, enter the IP address of the secondary DNS server.
- **WINS 1:** Optionally, enter the IP address of the primary WINS server.
- **WINS 2:** Optionally, enter the IP address of the secondary WINS server.
- **Domain Name:** Optionally, enter the domain name for the DMZ.
- **Default Gateway:** Enter the IP address of default gateway.
- **Option 66:** Provides provisioning server address information to hosts requesting this option. Only supports the IP address or host name of a single TFTP server. Enter the IP address of the single TFTP server for the DMZ.
- **Option 67:** Provides a configuration/bootstrap file name to the hosts requesting this option. This is used in conjunction with the option 66 to allow the client to form an appropriate TFTP request for the file. Enter the configuration/bootstrap file name on the specified TFTP server.
- **Option 150:** Supports a list of TFTP servers (2 TFTP servers). Enter the IP addresses of TFTP servers. Separate multiple entries with commas (,).

STEP 5 In the **IPv6 Setting** tab, specify IPv6 addressing for the DMZ if you enable the IPv4/IPv6 mode.

- **IPv6 Address:** Enter the IPv6 address based on your network requirements.
- **IPv6 Prefix Length:** Enter the number of characters in the IPv6 prefix.

  The IPv6 network (subnet) is identified by the prefix, which consists of the initial bits of the address. The default prefix length is 64 bits. All hosts in the network have the identical initial bits for the IPv6 address. The number of common initial bits in the addresses is set by the prefix length field.

STEP 6 Click **OK** to save your settings.

STEP 7 Click **Save** to apply your settings.

STEP 8 If you want to reserve certain IP addresses for specified devices, go to the Networking > DHCP Reservations page. See **Configuring DHCP Reserved IPs, page 149**. You must enable DHCP Server or DHCP Relay mode for this purpose.

Configuring Zones

Use the Networking > Zones page to configure a security zone, which is a group of interfaces to which a security policy can be applied. The interfaces in a zone share common functions or features. For example, two interfaces that are connected to the local LAN might be placed in one security zone, and the interfaces connected to the Internet might be placed in another security zone.

The interfaces are IP-based interfaces (VLANs, WAN1, WAN2, and so forth). Each interface can only join one zone, but each zone with specific security level can have multiple interfaces.

Refer to the following topics:

- **Security Levels for Zones, page 146**
- **Predefined Zones, page 147**
- **Configuring Zones, page 147**

NOTE We recommend that you configure the zones before you configure WAN, VLAN, DMZ, zone-based firewall, and security services.

Security Levels for Zones

The security level for the zone defines the level of trust given to that zone. The security appliance supports five security levels for the zones as described below. The greater value, the higher the permission level. The predefined VPN and SSLVPN zones have the same security level.

- **Trusted(100):** Offers the highest level of trust. The LAN zone is always trusted.
- **VPN(75):** Offers a higher level of trust than a public zone, but a lower level of trust than a trusted zone, which is used exclusively by the predefined VPN and SSLVPN zones. All traffic to and from a VPN zone is encrypted.
- **Public(50):** Offers a higher level of trust than a guest zone, but a lower level of trust than a VPN zone. The DMZ zone is a public zone.
- **Guest(25):** Offers a higher level of trust than an untrusted zone, but a lower level of trust than a public zone. Guest zones can only be used for guest access.

- **Untrusted(0):** Offers the lowest level of trust. It is used by both the WAN and the virtual multicast zones. You can map the WAN port to an untrusted zone.

Predefined Zones

The security appliance predefines the following zones with different security levels:

- **WAN:** The WAN zone is an untrusted zone. By default, the WAN1 port is mapped to the WAN zone. If the secondary WAN (WAN2) is applicable, it can be mapped to the WAN zone or any other untrusted zone.
- **LAN:** The LAN zone is a trusted zone. You can map one or multiple VLANs to a trusted zone. By default, the DEFAULT VLAN is mapped to the LAN zone.
- **DMZ:** The DMZ zone is a public zone used for the public servers that you host in the DMZ networks.
- **SSLVPN:** The SSLVPN zone is a virtual zone used for simplifying secure and remote SSL VPN connections. This zone does not have an assigned physical port.
- **VPN:** The VPN zone is a virtual zone used for simplifying secure IPsec VPN connections. This zone does not have an assigned physical port.
- **GUEST:** The GUEST zone can only be used for guest access. By default, the GUEST VLAN is mapped to this zone.
- **VOICE:** The VOICE zone is a security zone designed for voice traffic. Traffic coming and outgoing from this zone will be optimized for voice operations. If you have voice devices, such as Cisco IP Phone, it is desirable to place the devices into the VOICE zone.

Configuring Zones

This section describes how to configure the zones on the security appliance. You can restore the zone configuration to the factory default settings, edit the settings of the predefined zones (except for the VPN and SSLVPN zones), or customize new zones for your specific business needs.

NOTE You can click **Reset** to restore your zone configuration to the factory default settings. All custom zones will be removed and the settings relevant to these custom zones will be cleaned up after you perform this operation.

STEP 1 To add a new zone, click **Add**. To edit an entry, click the **Edit** (pencil) icon.

Other options: To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

NOTE: All predefined zones (except for the VOICE zone) cannot be deleted. Only the associated ports and VLANs for the predefined zones (except for the VPN and SSLVPN zones) can be edited.

STEP 2 Enter the following information:

- **Name:** Enter the name for the zone.
- **Security Level:** Specify the security level for the zone.
  - For VLANs, all security levels are selectable.
  - For DMZs, choose Public(50).
  - For WAN ports, choose Untrusted(0).
- **Map interfaces to this zone:** Choose the existing VLANs or WAN ports from the **Available Interfaces** list and click the right arrow to add them to the **Mapped to Zone** list. Up to 16 VLANs can be mapped to a zone.

STEP 3 Click **OK** to save your settings and close the pop-up window.

STEP 4 Click **Save** to apply your settings.

NOTE Next steps:

- After you create a new zone, a certain amount of firewall rules will be automatically generated to permit or block traffic from the new zone to other zones or from other zones to the new zone. The permit or block action is determined by the security level of the new zone. By default, the firewall prevents all inbound traffic and allows all outbound traffic. To customize firewall rules for the new zone, go to the Firewall > Access Control > ACL Rules page. For information on configuring firewall rules, see Configuring Firewall Rules to Control Inbound and Outbound Traffic, page 252.
- Apply the security services on the zones if you enable the security services such as Intrusion Prevention (IPS), Anti-Virus, and Application Control on the security appliance. For complete details, see **Chapter 7, "Security Services."**

Configuring DHCP Reserved IPs

Use the Networking > DHCP Reservations page to reserve certain IP addresses for specified devices, identified by their MAC addresses. Whenever the DHCP server receives a request from a device, the hardware address is compared with the database. If the device is found, then the reserved IP address is used. Otherwise, an IP address is assigned automatically from the DHCP pool.

STEP 1 To add a DHCP Reservation rule, click **Add**. To edit an entry, click the **Edit** (pencil) icon.

Other options: To delete an entry, click the **Delete** (x) icon.

The DHCP IP Reservation- Add/Edit window opens.

STEP 2 Enter the following information:

- **Name:** Enter the name for the DHCP Reservation rule.
- **MAC Address:** Enter the MAC address of the host under a VLAN.
- **IP Address:** Enter the IP address that is assigned to the host. The address must be within the DHCP pool of the VLAN.

STEP 3 Click **OK** to save your settings and close the pop-up window.

STEP 4 Click **Save** to apply your settings.

Configuring Routing

This section provides information on configuring the routing mode between WAN and LAN, viewing the routing table, and configuring the static routing, dynamic routing, and Policy-Based Routing settings. Refer to the following topics:

- **Viewing the Routing Table, page 150**
- **Configuring Routing Mode, page 150**
- **Configuring Static Routing, page 151**
- **Configuring Dynamic Routing - RIP, page 152**
- **Configuring Policy-Based Routing, page 153**

Viewing the Routing Table

Use the **Networking > Routing > Routing Table** page to view the following information:

- **Destination Address:** The IP address of the host or the network that the route leads to.
- **Subnetwork Mask:** The subnet mask of the destination network.
- **Gateway:** The IP address of the gateway through which the destination host or network can be reached.
- **Flags:** The status flag of the route.
- **Metric:** The cost of a route. Routing metrics are assigned to routes by routing protocols to provide measurable values that can be used to judge how useful (or how low cost) a route will be.
- **Interface:** The physical port through which this route is accessible.

This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the routing table.

Configuring Routing Mode

Use the **Networking > Routing > Routing Mode** page to enable or disable routing mode, based on the requirements of your ISP. By default, routing mode is disabled.

STEP 1 Enable or disable routing mode:

- If your ISP assigns an IP address for each of the computers that you use, click **On** to enable the Routing mode.
- If you are sharing IP addresses across several devices such as your LAN and using other dedicated devices for the DMZ, click **Off** to disable the Routing mode.

STEP 2 Click **Save** to apply your settings.

Configuring Static Routing

Use the Networking > Routing > Static Routing page to configure static routes. You can optionally assign a priority, which determines the route is selected when there are multiple routes travelling to the same destination.

NOTE Up to 150 static routing rules can be configured on the security appliance.

STEP 1 To add a static route, click **Add**. To edit an entry, click the **Edit** (pencil) icon.

Other options: To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

STEP 2 Enter the following information:

- **Destination Address:** Choose an existing address object for the host or for the network that the route leads to. If the address object that you want is not in the list, choose **Create a new address** to create a new address object. To maintain the address objects, go to the Networking > Address Management page. See **Address Management, page 175**.
- **Setting as default route:** Check this box to set this static route as the default route.
- **Next Hop:** Choose a port or an IP address as the next hop for this static route.
  - **Interface:** Choose either WAN1 or WAN2 as the next hop.
  - **IP Address:** Choose an IP address of the gateway through which the destination host or network can be reached.
- **Metric:** Optionally, enter a number to manage the route priority. If multiple routes to the same destination exist, the route with the lowest metric is selected.

STEP 3 Click **OK** to save your settings and close the pop-up window.

STEP 4 Click **Save** to apply your settings.

Configuring Dynamic Routing - RIP

Use the Networking > Routing > Dynamic - RIP page to configure Dynamic Routing or RIP. RIP is an Interior Gateway Protocol (IGP) that is commonly used in internal networks. It allows a router to exchange its routing information automatically with other routers, and allows it to dynamically adjust its routing tables and adapt to changes in the network.

STEP 1 At the top of the page, enter the following information:

- **RIP Enable:** Click **On** to enable RIP, or click **Off** to disable it. By default, RIP is disabled.
- **RIP Version:** If you enable RIP, specify the RIP version. The security appliance supports RIP Version 1 and RIP Version 2.
  - **RIP Version 1** is a class-based routing version that does not include subnet information. This is the most commonly supported version.
  - **RIP Version 2** includes all the functionality of RIPv1 plus it supports subnet information.
  - **Default:** The data is sent in RIP Version 1 format and received in RIP Version 1 and 2 format. This is the default setting.

STEP 2 In the table, specify the RIP settings for each available interface:

- **RIP Enable:** Check this box to enable the RIP settings on the port or VLAN.
- **Authentication:** If you are using RIP Version 2, click the **Edit** (pencil) icon to specify the authentication method for the port or VLAN.
  - **None:** Choose this option to invalidate the authentication.
  - **Simple Password Authentication:** Choose this option to validate the simple password authentication. Enter the password in the field.
  - **MD5 Authentication:** Choose this option to validate the MD5 authentication. Enter the unique key ID in the **MD5 Key ID** field and the Key in the **MD5 Auth Key** field.
- **Port Passive:** Determines how the security appliance receives RIP packets. Check this box to enable this feature on the port or VLAN.

STEP 3 Click **Save** to apply your settings.

Configuring Policy-Based Routing

Use the Networking > Routing > Policy Based Routing page to configure Policy-Based Routing (PBR). PBR specifies the internal IP and/or service going through a WAN port to provide more flexible and granular traffic handling capabilities. Up to 100 Policy-Based Routing rules can be configured on the security appliance.

This feature can be used to segregate traffic between links that are not of the same speed. High volume traffic can be routed through the port connected to a high speed link and low volume traffic can be routed through the port connected to the slow link. For example, although HTTP traffic is typically routed through WAN1, by using PBR you can bind the HTTP protocol to WAN1 and bind the FTP protocol to WAN2. In this case, the security appliance automatically channels FTP data through WAN2.

If multiple routing features operate simultaneously, the security appliance first matches the Policy-Based Routing rules, and then matches the Static Routing and default routing rules. For example, if the WAN redundancy is set as the Weighted Dual WAN Settings and the Policy-Based Routing and Static Routing rules are configured, the routing priority works as follows:

1. If traffic cannot match the Policy-Based Routing or Static Routing rules, traffic follows the Weighted Dual WAN Settings.
2. If traffic A matches the Policy-Based Routing or Static Routing rules, it will first be handled by the Policy-Based Routing or Static Routing rules, while other traffic follows the Weighted Dual WAN Settings.

NOTE Make sure that you configure a secondary WAN connection and that the WAN redundancy is set to Dual WAN Settings or Routing Table mode before you configure the Policy-Based Routing settings.

STEP 1 Click **On** to enable PBR, or click **Off** to disable it.

STEP 2 To add a new PBR rule, click **Add**. To edit an entry, click the **Edit** (pencil) icon.

Other options: To delete an entry, click the **Delete** (x) icon.

STEP 3 Enter the following information:

- **From:** Choose the VLAN that traffic originates from.
- **Service:** For service binding only, choose an existing service. For IP binding only, choose **All Traffic**. If the service that you want is not in the list, choose **Create a new service** to create a new service object. To maintain the service objects, go to the Networking > Service Management page. See **Service Management, page 177**.
- **Source IP:** For service binding only, choose **Any**. For IP binding only, choose the source IP address for outbound traffic. If the address object that you want is not in the list, choose **Create a new address** to create a new address object. To maintain the address objects, go to the Networking > Address Management page. See **Address Management, page 175**.
- **Destination IP:** For service binding only, choose **Any**. For IP binding only, choose the destination IP address for outbound traffic.
- **DSCP:** Choose the DSCP value to assign the traffic priority.
- **Route to:** Choose the WAN port that outbound traffic routes to.
- **Failover:** Click **On** to enable WAN Failover, or click **Off** to disable it. When the selected WAN port for routing is down, enabling Failover will forward traffic to the backup WAN.

  NOTE: When one WAN connection is down (a connection failure is detected by ping or DNS query) and the Failover feature of PBR is disabled, traffic will be dropped.

STEP 4 Click **OK** to save your settings and close the pop-up window.

STEP 5 Click **Save** to apply your settings.

NOTE: After you apply your settings, the modified PBR settings will take effect immediately for any new sessions, but not for the existing sessions. You can manually clear the existing sessions on the Firewall > Session Limits page to apply the PBR settings immediately for all new sessions.

Configuring Quality of Service

The Quality of Service (QoS) feature is applied throughout the network to ensure that network traffic is prioritized according to required criteria and that the desired traffic receives preferential treatment.

QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP, online games, and IPTV, since these applications are delay sensitive and often require a fixed bit rate.

Refer to the following topics:

- General QoS Settings, page 155
- Configuring WAN QoS, page 156
- Configuring LAN QoS, page 166
- Configuring Wireless QoS, page 169
- Understanding DSCP Values

General QoS Settings

Use the General Settings page to enable or disable the WAN QoS, LAN QoS, and WLAN QoS features.

STEP 1 Click **Networking > QoS > General Settings**.

STEP 2 Enter the following information:

- **WAN QoS:** Check this box to enable WAN QoS. By default, WAN QoS is disabled.
- **LAN QoS:** Check this box to enable LAN QoS. LAN QoS specifies priority values that can be used to differentiate traffic and give preference to higher-priority traffic, such as telephone calls. By default, LAN QoS is disabled.
- **Wireless QoS:** Check this box to enable Wireless QoS. Wireless QoS controls priority differentiation for data packets in wireless egress direction. By default, Wireless QoS is disabled. The wireless QoS only applies to the ISA550W and ISA570W.

STEP 3 Click **Save** to apply your settings.

Configuring WAN QoS

This section describes how to configure WAN QoS. Refer to the following topics:

- **Managing WAN Bandwidth for Upstream Traffic, page 156**
- **Configuring WAN Queue Settings, page 157**
- **Configuring Traffic Selectors, page 158**
- **Configuring WAN QoS Policy Profiles, page 160**
- **Configuring WAN QoS Class Rules, page 160**
- **Mapping WAN QoS Policy Profiles to WAN Interfaces, page 161**
- **WAN QoS Configuration Example, page 162**
- **Configure WAN QoS for Voice Traffic from LAN to WAN, page 164**
- **Configuring WAN QoS for Voice Traffic from WAN to LAN, page 165**

Managing WAN Bandwidth for Upstream Traffic

Use the Bandwidth page to specify the maximum bandwidth for upstream traffic allowed on each WAN interface.

STEP 1 Click **Networking > QoS > WAN QoS > Bandwidth**.

STEP 2 Enter the amount of maximum bandwidth for upstream traffic allowed on each WAN interface. The default value is 6000 Kbps, which indicates that there is no limit for upstream traffic.

STEP 3 Click **Save** to apply your settings.

Configuring WAN Queue Settings

Use the Queue Settings page to determine how traffic in queues is handled for each WAN port. The security appliance supports six queues for the WAN ports, Q1 to Q6. There are three ways of determining how traffic in queues is handled:

Strict Priority (SP)	Egress traffic from the highest-priority queue (Q1) is transmitted first. Traffic from the lower queues is processed only after the highest queue has been transmitted, thus providing the highest level of priority of traffic to the highest numbered queue.
Weighted Round Robin (WRR)	Distributes the bandwidth between the classes using the weighted round robin scheme. The weights decide how fast each queue can send packets. In WRR mode the number of packets sent from the queue is proportional to the weight of the queue. The higher the weight, the more frames are sent.
Low Latency Queuing (LLQ)	The default setting, Low Latency Queuing (LLQ) allows delay-sensitive data (such as voice) to be given preferential treatment over other traffic by sending it first. You can enter the PQ for Q1 and a description for each queue. By default the PQ is 1200 Kbps. The Queue Descriptions are: Q1—Voice traffic Q2—Signaling Q3—Routing/VPN control Q4—Management Q5—Video Q6—Best Effort

STEP 1 Click **Networking > QoS > WAN QoS > Queue Settings**.

STEP 2 Specify the way of determining how traffic in queues is handled for each WAN port.

- **Strict Priority (SP):** Set the order in which queues are serviced, traffic scheduling for the selected queue and all higher queues is based strictly on the queue priority, starting with Q1 (the highest priority queue) and going to the next lower queue when each queue is complete.
- **Weighted Round Robin (WRR):** Enter the WRR weight, in percentage, assigned to the queues that you want to use. Traffic scheduling for the selected queue is based on WRR.
- **Low Latency Queuing (LLQ):** Apply SP mode to Q1 and WRR mode to other queues (Q2 to Q6). Q1 has the highest priority and is always processed to completion before the lower priority queues. If you choose LLQ, enter the amount of bandwidth assigned to Q1, and enter the WRR weights for other queues that you want to use.

STEP 3 If needed, enter a brief description for each queue in the field in the **Queue Description** column.

STEP 4 In the **Random Early Detection** area, click **On** to enable the Random Early Detection (RED) mechanism, or click **Off** to disable RED. RED is a congestion avoidance mechanism that takes advantage of TCP's congestion control mechanism. By randomly dropping packets prior to periods of high congestion, RED tells the packet source to decrease its transmission rate. Assuming the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, indicating that the congestion is cleared.

STEP 5 Click **Save** to apply your settings.

Configuring Traffic Selectors

Traffic Selector (or Traffic Classification) is used to classify traffic through WAN interfaces to a given traffic class so that traffic in need of management can be identified.

NOTE Up to 256 traffic selectors can be configured on the security appliance.

STEP 1 Click **Networking > QoS > WAN QoS > Traffic Selector (Classification)**.

The Traffic Selector (Classification) window opens.

STEP 2 To add a new traffic selector, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon.

The Traffic Selector - Add/Edit window opens.

STEP 3 Enter the following information:

- **Class Name:** Enter a descriptive name for the traffic class.
- **Source Address:** Choose **Any** or choose an existing address or address group (network) that traffic comes from.
- **Destination Address:** Choose **Any** or choose an existing address or address group (network) that traffic goes to.

  If the address objects that you want are not in the list, choose **Create a new address group** to create a new address group object or choose **Create a new address** to create a new address object. To maintain the address or address group objects, go to the Networking > Address Management page. See **Address Management, page 175**.
- **Source Service:** Choose **Any** or choose an existing service from the drop-down list.
- **Destination Service:** Choose **Any** or choose an existing service from the drop-down list.

  If the service objects that you want are not in the list, choose **Create a new service** to create a new service object. To maintain the service objects, go to the Networking > Service Management page. See **Service Management, page 177**.
- **DSCP:** DSCP is a field in an IP packet that enables different levels of service to be assigned to network traffic. Select the DSCP values for the traffic class and click the right arrow. For more information, see **Understanding DSCP Values, page 171**.
- **CoS:** QoS-based IEEE 802.1p Class of Service (CoS) specifies a priority value of between 0 and 7 that can be used to differentiate traffic and give preference to higher-priority traffic. Choose the CoS value for the traffic class.
- **VLAN:** Choose the VLAN for identifying the host to which the traffic selector will apply.

NOTE: Traffic that matches the above settings will be classified to a class for management purposes.

STEP 4 Click **Save** to apply your settings.

Configuring WAN QoS Policy Profiles

Use the QoS Policy Profile page to configure class-based policy profiles for managing traffic through the WAN interfaces.

NOTE Up to 32 WAN QoS policy profiles can be configured on the security appliance.

STEP 1 Click **Networking > QoS > WAN QoS > QoS Policy Profile**.

STEP 2 To add a new WAN QoS policy profile, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon.

The QoS Policy - Add/Edit window opens.

STEP 3 Enter the following information:

- **Policy Name:** Enter the name for the WAN QoS policy profile.
- **Apply this policy to:** Click **Inbound Traffic** to apply this policy profile for inbound traffic, or click **Outbound Traffic** to apply this policy profile for outbound traffic.

STEP 4 Specify the QoS settings for the traffic classes that you want to associate with the policy profile. For complete details, see **Configuring WAN QoS Class Rules, page 160**.

STEP 5 Click **OK** to save your settings.

STEP 6 Click **Save** to apply your settings.

Configuring WAN QoS Class Rules

This section describes how to configure the QoS class rules that you want to associate with the WAN QoS policy profile.

NOTE Up to 64 traffic classes can be associated with one WAN QoS policy profile.

STEP 1 In the **QoS Class Rules** area, click **Add** to add a WAN QoS class rule.

The QoS Class Rule - Add/Edit window opens.

STEP 2 Enter the following information:

- **Class:** Choose an existing traffic selector (traffic class) to associate with the policy profile.
- **Queue:** For an outbound traffic policy profile, choose the queue for sending the packets that belongs to the selected traffic class. This option will be disabled for an inbound traffic policy profile.
- **DSCP Marking:** Choose the DSCP remarking value to assign the priority for traffic. For more information, see **Understanding DSCP Values, page 171**.
- **CoS Marking:** For an inbound traffic policy profile, choose the CoS remarking value to assign the priority for inbound traffic. This option will be disabled for an outbound traffic policy profile.
- **Rate-limiting:** Enter the amount of bandwidth limitation in Kbps for the selected traffic class. For example, if the policy profile is applied to inbound traffic, the rate-limiting setting only applies to incoming traffic that belongs to the selected class. The default value is 0 Kbps, which indicates that there is no limit.

STEP 3 Click **OK** to save your settings.

Mapping WAN QoS Policy Profiles to WAN Interfaces

Use the Policy Profile to Interface Mapping page to apply the WAN QoS policy profiles on the WAN interfaces.

STEP 1 Click **Networking > QoS > WAN QoS > Policy Profile to Interface Mapping**.

The Policy Profile to Interface Mapping window opens.

STEP 2 To edit the policy profile settings associated with a WAN interface, click the **Edit** (pencil) icon.

The Policy Profile to Interface Mapping - Edit window opens.

STEP 3 Enter the following information:

- **Interface:** The name of the WAN interface with which the policy profiles are associated.
- **Inbound Policy Name:** Choose an inbound policy profile for managing inbound traffic through the selected WAN interface.
- **Outbound Policy Name:** Choose an outbound policy profile for managing outbound traffic through the selected WAN interface.

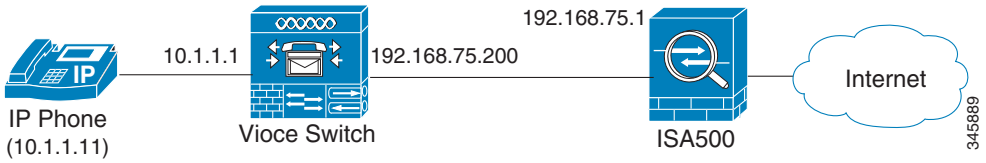
STEP 4 Click **OK** to save your settings.

STEP 5 Click **Save** to apply your settings.

WAN QoS Configuration Example

This section provides a configuration example on setting up WAN QoS to give the voice traffic a higher priority for a phone system or the SPA phones through the security appliance.

Use Case: An IP phone is connected directly to the voice switch behind the security appliance or the LAN port the security appliance. Both voice and data traffic is sent out through the WAN port of the security appliance.



Solution: For the voice traffic from LAN to WAN (outbound voice traffic), make sure that the outbound voice traffic is handled by the highest priority queue (Q1) and other outbound traffic such as data traffic is handled by the lower priority queues (Q2 to Q6). For the voice traffic from WAN to LAN (inbound voice traffic), CoS and DSCP will be remarked so that the voice switch can prioritize the inbound voice traffic by incoming CoS or DSCP.

Perform the following configuration tasks to give the voice traffic a higher priority:

- Go to the Networking > Routing > Static Routing page to add a static routing rule as follows:

Destination Address	voice_phone_ip **NOTE:** In this case, you can manually create an IP address object called “voice_phone_ip” with the IP address 10.1.1.11 by selecting the **Create a new address** option.
IP Address	voice_switch_ip **NOTE:** In this case, you can manually create an IP address object called “voice_switch_ip” with the IP address 192.168.75.200 by selecting the **Create a new address** option.
Metric	1

- Go to the Firewall > NAT > Advanced NAT page to add an advanced NAT rule as follows to permit the voice and data traffic through the WAN port (WAN1) of the security appliance:

Name	voice_traffic_nat
Enable	On
From	Any
To	WAN1
Original Source Address	voice_phone_ip
Translated Source Address	WAN1_IP

- Go to the Networking > QoS > General Settings page to enable WAN QoS on the security appliance.
- Go to the Networking > QoS > WAN QoS > Bandwidth page to specify the upstream bandwidth for the WAN port.
- Configure WAN QoS for the outbound voice traffic. For complete details, see **Configure WAN QoS for Voice Traffic from LAN to WAN, page 164**.

- Configure WAN QoS for the inbound voice traffic. For complete details, see **Configuring WAN QoS for Voice Traffic from WAN to LAN, page 165**.

Configure WAN QoS for Voice Traffic from LAN to WAN

Follow these steps to configure WAN QoS to manage the outbound voice traffic from LAN to WAN:

STEP 1 Go to the Networking > QoS > WAN QoS > Queue Settings page to determine how traffic in queues is handled for the WAN port.

a. Select the **Low Latency Queuing (LLQ)** radio button. LLQ allows delay-sensitive data (such as voice traffic) to be given preferential treatment over other traffic by letting the data to be de-queued and sent first.

a. Enter the amount of bandwidth assigned to Q1. Q1 has the highest priority and is always processed to completion before the lower priority queues.

b. Enter the percentage assigned to other queues (Q2 to Q6) that you want to use.

STEP 2 Go to the Networking > QoS > WAN QoS > Traffic Selector (Classification) page to add two traffic selectors used to classify the outbound voice and data traffic.

a. Add a traffic selector as follows to classify the outbound data traffic:

Class Name	data-outbound-class
VLAN	Default VLAN

b. Add a traffic selector as follows to classify the outbound voice traffic:

Class Name	voice-outbound-class
Source Address	voice_phone_ip

STEP 3 Go to the Networking > QoS > WAN QoS > QoS Policy Profile page to add a class-based QoS policy profile to manage the outbound voice and data traffic through the WAN port.

a. Add a WAN QoS policy profile as follows:

Policy Name	voice-outbound-profile
Apply this policy to	Outbound Traffic

b. Add two QoS class rules to associate the specified traffic classes with the QoS policy profile as follows:

QoS Class Rule 1	
Class	Choose the traffic class called "voice-outbound-class."
Queue	Choose the highest queue Q1 for the outbound voice traffic.
QoS Class Rules 2	
Class	Choose the traffic class called "data-outbound-class."
Queue	Choose one queue from Q2 to Q6 for the outbound data traffic.

STEP 4 Go to the Networking > QoS > WAN QoS > Policy Profile to Interface Mapping page to apply this QoS policy profile on the WAN port. In this case, choose the QoS policy profile called "voice-outbound-profile" from the **Outbound Policy Name** drop-down list.

Configuring WAN QoS for Voice Traffic from WAN to LAN

Follow these steps to configure WAN QoS to manage the inbound voice traffic from WAN to LAN:

STEP 1 Go to the Networking > QoS > WAN QoS > Traffic Selector (Classification) page to add a traffic selector as follows to classify the inbound voice traffic:

Class Name	voice-inbound-class
Destination Address	voice_phone_ip

STEP 2 Go to the Networking > QoS > WAN QoS > QoS Policy Profile page to add a class-based QoS policy profile as follows to manage the inbound voice traffic through the WAN port:

Policy Name	voice-inbound-profile
Apply this policy to	Inbound Traffic

QoS Class Rule	Add a QoS class rule with the following settings: ▪ **Class:** Choose the traffic class called "voice-inbound-class." ▪ **DSCP Marking:** Choose the DSCP tag value (such as 46) for the inbound voice traffic depending on the QoS settings on your voice switch. For more information, see **Understanding DSCP Values, page 171**. ▪ **CoS Marking:** Choose the CoS tag value (such as 6) for the inbound voice traffic depending on the QoS settings on your voice switch.

STEP 3 Go to the Networking > QoS > WAN QoS > Policy Profile to Interface Mapping page to apply the inbound QoS policy profile on the WAN port. In this case, choose the QoS policy profile called "voice-inbound-profile" from the **Inbound Policy Name** drop-down list.

Configuring LAN QoS

LAN QoS specifies priority values that can be used to differentiate traffic and give preference to higher-priority traffic, such as telephone calls. Refer to the following topics:

- **Configuring LAN Queue Settings, page 167**
- **Configuring LAN QoS Classification Methods, page 167**
- **Mapping CoS to LAN Queue, page 168**
- **Mapping DSCP to LAN Queue, page 168**
- **Configuring Default CoS, page 169**

Configuring LAN Queue Settings

Use the Queue Settings page to configure whether traffic scheduling on Ethernet interfaces is based on either SP or WRR, or the combination of the two. The security appliance supports four queues for LAN traffic, Q1 to Q4.

STEP 1 Click **Networking > QoS > LAN QoS > Queue Settings**.

STEP 2 Specify how to determine LAN traffic in queues.

- **Strict Priority (SP):** Indicates that traffic scheduling for the selected queue is based strictly on the queue priority.
- **Weighted Round Robin (WRR):** Indicates that traffic scheduling for the selected queue is based strictly on the WRR weights. If WRR is selected, the predefined weights 8, 4, 2 and 1 are assigned to queues 1, 2, 3 and 4 respectively.
- **SP and WRR:** Integrates the SP and WRR queues. It applies SP to Q1 and WRR to other queues (Q2 to Q4). If you choose SP+WRR, the PQ is assigned to Q1 and the predefined weights 4, 2 and 1 are assigned to Q2, Q3, and Q4 respectively. There is no limit for PQ, indicating that WRR queues may be starved if PQ is always sending traffic greater than the maximum bandwidth of the LAN ports.

STEP 3 If needed, enter the description for each queue in the field in the **Queue Description** column.

STEP 4 Click **Save** to apply your settings.

Configuring LAN QoS Classification Methods

Traffic Classification is used to classify traffic through the LAN interfaces to a given traffic class so that traffic in need of management can be identified.

STEP 1 Click **Networking > QoS > LAN QoS > Classification Methods**.

STEP 2 Depending on your networking design, choose either Differentiated Services Code Point (DSCP) or Class of Service (CoS) remarking method for traffic through all LAN interfaces. When you choose DSCP as the classification method, the Mapping CoS to LAN Queue feature will be grayed out. In this case, the mapping relationship between LAN queues and CoS is defined as follows:

LAN Queue	CoS Value
1	6
2	4
3	2
4	0

STEP 3 Click **Save** to apply your settings.

Mapping CoS to LAN Queue

STEP 1 Click **Networking > QoS > LAN QoS > Mapping CoS to Queue**.

STEP 2 Choose the traffic forwarding queue to which the CoS priority tag value is mapped. Four traffic priority queues are supported, where Q4 is the lowest and Q1 is the highest.

STEP 3 Click **Save** to apply your settings.

Mapping DSCP to LAN Queue

STEP 1 Click **Networking > QoS > LAN QoS > Mapping DSCP to Queue**.

STEP 2 Choose the traffic forwarding queue to which the DSCP priority tag value is mapped. Four traffic priority queues are supported, where Q4 is the lowest and Q1 is the highest. For more information, see **Understanding DSCP Values, page 171**.

STEP 3 Click **Save** to apply your settings.

Configuring Default CoS

Use the Default CoS page to configure the default CoS values for incoming packets through each LAN interface. The possible field values are 0 to 7. The default value is 0.

STEP 1 Click **Networking > QoS > LAN QoS > Default CoS**.

STEP 2 Enter the following information:

- **Default CoS:** Choose the default CoS priority tag value for the LAN interfaces, where 0 is the lowest and 7 is the highest.
- **Trust:** Choose **Yes** to keep the CoS tag value for packets through the LAN interfaces, or choose **No** to change the CoS tag value for packets through the LAN interfaces.

STEP 3 Click **Save** to apply your settings.

Configuring Wireless QoS

Wireless QoS controls priority differentiation for data packets in wireless egress direction. Refer to the following topics:

- Default Wireless QoS Settings, page 169
- Configuring Wireless QoS Classification Methods, page 170
- Mapping CoS to Wireless Queue, page 171
- Mapping DSCP to Wireless Queue, page 171

Default Wireless QoS Settings

Wireless QoS uses the default queuing method for wireless traffic. Wireless traffic is always trusted. The following tables display the default mapping settings between 802.1p and 802.1e.

802.1p to IEEE 802.11e Mapping

802.1p Priority	802.11e Priority
0	0 (Best Effort Priority)

802.1p Priority	802.11e Priority
1	1 (Background Priority)
2	2 (Background Priority)
3	4 (Video Priority)
4	5 (Video Priority)
5	6 (Voice Priority)
6	7 (Voice Priority)
7	7 (Voice Priority)

IEEE 802.11e to 802.1p Mapping

802.11e Priority	802.1p Priority
0 (Best Effort Priority)	0
1 (Background Priority)	1
2 (Background Priority)	2
3 (Best Effort Priority)	0
4 (Video Priority)	3
5 (Video Priority)	4
6 (Voice Priority)	5
7 (Voice Priority)	6

Configuring Wireless QoS Classification Methods

Traffic Classification is used to classify traffic through the SSIDs to a given traffic class so that traffic in need of management can be identified.

STEP 1 Click **Networking > QoS > Wireless QoS > Classification Methods**.

STEP 2 Depending on your networking design, choose either DSCP or CoS remarking method for traffic through each SSID.

STEP 3 Click **Save** to apply your settings.

Mapping CoS to Wireless Queue

STEP 1 Click **Networking > QoS > Wireless QoS > Mapping CoS to Queue**.

STEP 2 Choose the traffic forwarding queue to which the CoS priority tag value is mapped.

STEP 3 Click **Save** to apply your settings.

Mapping DSCP to Wireless Queue

STEP 1 Click **Networking > QoS > Wireless QoS > Mapping DSCP to Queue**.

STEP 2 Choose the traffic forwarding queue to which the DSCP priority tag value is mapped. For more information, see **Understanding DSCP Values, page 171**.

STEP 3 Click **Save** to apply your settings.

Understanding DSCP Values

DSCP Value	Decimal Value	Meaning
101 110	46	High Priority, Expedited Forwarding (EF)
000 000	0	Best Effort
001 010	10	AF11
001 100	12	AF12
001 110	14	AF13
010 010	18	AF21

DSCP Value	Decimal Value	Meaning
010 100	20	AF22
010 110	22	AF23
011 010	26	AF31
011 100	28	AF32
011 110	30	AF33
100 010	34	AF41
100 100	36	AF42
100 110	38	AF43

Configuring IGMP

Internet Group Management Protocol (IGMP) is a communication protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP can be used for online streaming video and gaming, and can allow more efficient use of resources when supporting these types of applications.

IGMP Proxy enables hosts that are not directly connected to a downstream router to join a multicast group sourced from an upstream network. IGMP Snooping constrains IPv4 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv4 multicast traffic only to those ports that want to receive it. IGMP Snooping runs on IGMP Version 3 that is backward compatible with the previous versions.

NOTE By default, multicast traffic from Any zone to Any zone is blocked by the firewall. When you enable IGMP Proxy and want to receive multicast packets from WAN to LAN, you must first uncheck **Block Multicast Packets** in the Firewall > Attack Protection page, and then create a firewall rule to permit multicast traffic from WAN to LAN. For information on configuring firewall rules to allow or deny multicast traffic, see Configuring a Firewall Rule to Allow Multicast Traffic, page 259.

STEP 1 Click **Networking > IGMP**.

The IGMP window opens.

STEP 2 Enter the following information:

- **IGMP Proxy:** Click **On** to enable IGMP Proxy so that the security appliance can act as a proxy for all IGMP requests and communicate with the IGMP servers of the ISP, or click **Off** to disable it.
- **IGMP Version:** Choose either IGMP Version 1 and 2 or IGMP Version 3.
  - **IGMP Version 1:** Hosts can join multicast groups. There are no leave messages. Routers use a time-out based mechanism to discover the groups that are of no interest to the members.
  - **IGMP Version 2:** Leave messages are added to the protocol. This allows group membership termination to be quickly reported to the routing protocol, which is important for high-bandwidth multicast groups and/or subnets with highly volatile group membership.
  - **IGMP Version 3:** Major revision of the protocol. It allows hosts to specify the lists of hosts from which they want to receive traffic. Traffic from other hosts is blocked inside the network. It also allows hosts to block packets inside the network that come from sources sending unwanted traffic.
- **IGMP Snooping:** Snooping streamlines multicast traffic handling for VLANs. By examining (snooping) IGMP membership report messages from interested hosts, multicast traffic is limited to the subset of VLAN interfaces on which the hosts reside. IGMP snooping can reduce bandwidth consumption to avoid flooding the entire VLAN. Click **On** to enable IGMP snooping, or click **Off** to disable it.

STEP 3 Click **Save** to apply your settings.

Configuring VRRP

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol for LAN access device. VRRP configures a groups of routers (include a master router and several backup routers) as a virtual router.

STEP 1 Click **Networking > VRRP**.

The VRRP window opens.

STEP 2 Check the box next to **Enable Virtual Router Redundancy Protocol (VRRP)** to enable VRRP, or uncheck this box to disable it.

STEP 3 If you enable VRRP, enter the following information:

- **Interface:** The default port of the master virtual router (your security appliance).
- **Source IP:** The source IP address of the master virtual router.

  NOTE: If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, this router will function as a master virtual router.
- **VRID:** The ID of the master virtual router. A virtual router has a unique ID that will be represented as the unique virtual MAC address. Enter a value from 1 to 255.
- **Priority:** The priority of the master virtual router. Priority determines the role that each VRRP router plays and what happens if the master virtual router fails. Enter a value from 1 to 254.
- **Advertisement Interval:** Specify the interval in seconds between successive advertisements by the master virtual router in a VRRP group. By default, the advertisements are sent every one second. The advertisements being sent by the master virtual router communicate the state and priority of the current master virtual router.

  NOTE: All routers in a VRRP group must use the same advertisement interval value. If the interval values are not same, the routers in the VRRP group will not communicate with each other and any mis-configured router will change its state to master.
- **Verify:** Click **On** to enable the authentication, or click **Off** to disable it. The security appliance will ignore incoming VRRP packets from routers that do not have the same authentication configuration for a VRRP group. VRRP supports the plaintext and IPsec-AH authentication schemes. Choose either Pass or AH as the authentication scheme and specify the settings.
- **Virtual IP Address:** Enter the virtual IP address used for all backup virtual routers in the same group.
- **Status:** Displays the status of VRRP verification.

STEP 4 Click **Save** to apply your settings.

Address Management

Use the Address Management page to manage the address and address group objects. The security appliance is configured with a long list of common address objects so that you can use to configure firewall rules, port forwarding rules, or other features. See Default Address Objects, page 478.

Refer to the following topics:

- **Configuring Addresses, page 175**
- **Configuring Address Groups, page 176**

Configuring Addresses

STEP 1 Click **Networking > Address Management**.

STEP 2 In the **Address Objects** area, click **Add Address** to add a new address object.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**. The default address objects cannot be edited and deleted.

The Address Object - Add/Edit window opens.

STEP 3 Enter the following information:

- **Name:** Enter the name for the address object.
- **Type:** Specify the address type and enter the corresponding information.
  - **Host:** Defines a single host by its IP address. The netmask for a Host address object will automatically be set to 32-bit (255.255.255.255) to identify it as a single host. If you choose Host, enter the IP address of the host in the **IP Address** field.
  - **Range:** Defines a range of contiguous IP addresses. No netmask is associated with the Range address object, but internal logic generally treats each member of the specified range as a 32-bit masked host object. If you choose Range, enter the starting IP address in the **Starting IP Address** field and the ending IP address in the **Ending IP Address** field.

- **Network:** Network address object like the Range object comprises multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask. Network address objects must be defined by the network's address and a corresponding netmask. As a general rule, the first address in a network (the network address) and the last address in a network (the broadcast address) are unusable. If you choose Network, enter the subnet IP address in the **IP Address** field and the broadcast address in the **Netmask** field.
- **MAC:** Identifies a host by its hardware address or MAC (Media Access Control) address. MAC addresses are uniquely assigned to wired or wireless networking devices by their hardware manufacturers. MAC addresses are 48-bit values that are expressed in 6 byte hex-notation. If you choose MAC, enter the MAC address in the **MAC** field.

STEP 4 Click **OK** to save your settings.

STEP 5 Click **Save** to apply your settings.

Configuring Address Groups

An address group object combines with multiple address objects. The security appliance supports up to 64 address group objects. An address group can include up to 100 address members.

STEP 1 Click **Networking > Address Management**.

STEP 2 In the **Address Groups** area, click **Add Group** to add a new address group object.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The Address Group - Add/Edit window opens.

STEP 3 Enter the name for the address group object in the **Group Name** field.

STEP 4 To add the address objects to the group, select the address objects from the left list and click the right arrow.

STEP 5 To remove the address objects from the group, select the address objects from the right list and click the left arrow.

STEP 6 Click **OK** to save your settings.

STEP 7 Click **Save** to apply your settings.

Service Management

Use the Service Management page to maintain the service or service group objects. The security appliance is configured with a long list of standard services so that you can use to configure the firewall rules, port forwarding rules, or other features. See Default Service Objects, page 474.

Refer to the following topics:

- **Configuring Services, page 177**
- **Configuring Service Groups, page 178**

Configuring Services

If you need to configure a feature for a custom service that is not in the standard list, you must first define the service object.

STEP 1 Click **Networking > Service Management**.

STEP 2 In the **Services** area, click **Add Service** to add a new service.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**. The default services cannot be deleted. Only the port range for the default services can be modified.

The Service Object - Add/Edit window opens.

STEP 3 Enter the following information:

- **Name:** Enter the name for the service.
- **Protocol:** Specify the protocol and port range for the service:
  - **IP:** Uses the predefined IP type. If you choose this option, enter the protocol number in the **IP Type** field.

- **ICMP:** Internet Control Message Protocol (ICMP) is a TCP/IP protocol used to send error and control messages. If you choose this option, enter the ICMP type in the **ICMP Type** field.
- **TCP:** Transmission Control Protocol (TCP) is a transport protocol in TCP/IP. TCP ensures that a message is sent accurately and in its entirety. If you choose this option, enter the starting port number in the **Port Range Start** field and the ending port number in the **Port Range End** field.
- **UDP:** User Datagram Protocol (UDP) is a protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required. If you choose this option, enter the starting port number in the **Port Range Start** field and the ending port number in the **Port Range End** field.
- **Both (TCP/UDP):** If you choose this option, enter the starting port number in the **Port Range Start** field and the ending port number in the **Port Range End** field.

STEP 4 Click **OK** to save your settings.

STEP 5 Click **Save** to apply your settings.

Configuring Service Groups

Services that apply to common applications are grouped as a service group object. The service group is treated as a single service. The security appliance supports up to 64 service groups. A service group can include up to 64 service members.

STEP 1 Click **Networking > Service Management**.

STEP 2 In the **Service Groups** area, click **Add Group** to add a new service group.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The Service Group - Add/Edit window opens.

STEP 3 Enter the name for the service group in the **Group Name** field.

STEP 4 To add the services to the group, select the services from the left list and click the right arrow.

STEP 5 To remove the services from the group, select the services from the right list and click the left arrow.

STEP 6 Click **OK** to save your settings.

STEP 7 Click **Save** to apply your settings.

Configuring Captive Portal

You may want to direct users to a web portal before they can access the Internet through the security appliance. To achieve this goal, you can enable Captive Portal on a wireless network, a VLAN, or a DMZ.

When a user in a Captive Portal user group attempts to access the Internet via a web browser, a portal page appears. You can require a log in or the entry of payment information, for example, and you can set up the portal page to display information, usage guidelines, warning messages, and so on. After successfully logging in, paying, or acknowledging your messages, the user can use other applications on the PC to communicate with the network.

In addition to the portal options mentioned above, additional options make it easy to adapt the Captive Portal feature to your needs:

- You can specify certain domains that users can access without going through the portal.
- The portal page can be stored locally on the ISA500 device or on an external web server that you specify.

Requirements

This feature is compatible with these browsers:

- Internet Explorer (v 8.0 or above)
- Firefox (v 9.0 or above)
- Google Chrome
- Safari

A computer accessing the Captive Portal must have one of these operating systems:

- Windows 7
- Windows XP
- Mac OS

Captive Portal also can be used from a mobile device with one of these operating systems:

- iOS (iPhone, iPad)
- Android

Before You Begin

Before you configure your portal, you may need to configure VLANs, SSIDs, and users. Read the following information to determine what steps may be needed to achieve your goals.

VLAN Setup

No special VLAN configuration is required for a Captive Portal, but you may want to consider the points below before proceeding. To configure VLANs, use the Networking > VLAN page..

- Each SSID is associated with a VLAN. You can use the pre-configured VLANs (DEFAULT, GUEST, and VOICE) or add a custom VLAN.
- You may want to associate a VLAN, such as the GUEST VLAN, with a security zone so that you can configure appropriate security policies. For example, you can apply URL filtering policies to the zone to prevent access to certain types of websites.
- A Captive Portal must be associated either with a single SSID or with a VLAN. If you want to enable a portal for users of multiple SSIDs, you will need to assign them all to the same VLAN. You can use a pre-configured VLAN or can create a VLAN for this purpose.

Wireless Setup

For a Captive Portal on the wireless network, you must enable the wireless radio and at least one SSID before you can enable a Captive Portal. To configure these settings, use the Wireless > Basic Settings page. .

- Enable the wireless radio.
- Enable the SSID(s) that you want to use for the portal.
- If you created a special VLAN for use with your Captive Portal, assign it to the SSID(s) that you want to use for the portal.

User Authentication

If you want to require user authentication for your portal, the security appliance can authenticate the users by using the local database and an external AAA server (such as RADIUS, AD, and LDAP). The authentication method is derived from the user authentication settings that you specified in the Users > User Authentication page. See Configuring User Authentication Settings, page 393.

For the local database option, you need to set up a User Group with the Captive Portal service enabled, and add the users' names and passwords. .

Configuring a Captive Portal

You configure this feature separately for the wireless network (**Wireless > Captive Portal**) and for the wired network (**Networking > Captive Portal**).

STEP 1 **Enable Captive Portal:** Click **On** to enable the Captive Portal feature.

STEP 2 **Apply On:** Choose the SSID, VLAN, or DMZ interface on which to apply the Captive Portal settings.

STEP 3 **Web Authentication Type:** Choose one of the following methods for web authentication. The security appliance can authenticate the users by using the local database and external AAA server (such as RADIUS, AD, and LDAP). The authentication method is derived from the user authentication settings that you specified in the Users > User Authentication page.

- **Internal:** Uses the default HotSpot Login page and requires a login.

- **Internal, no auth with accept button:** Uses the default HotSpot Login page and does not require a login. A user simply clicks the **Accept** button to access the Internet.
- **External:** Uses a custom HotSpot Login page on the specified external web server and requires a login.
- **External, no auth with accept button:** Uses a custom HotSpot Login page on the specified external web server and does not require a login. A user simply clicks the **Accept** button to access the Internet.

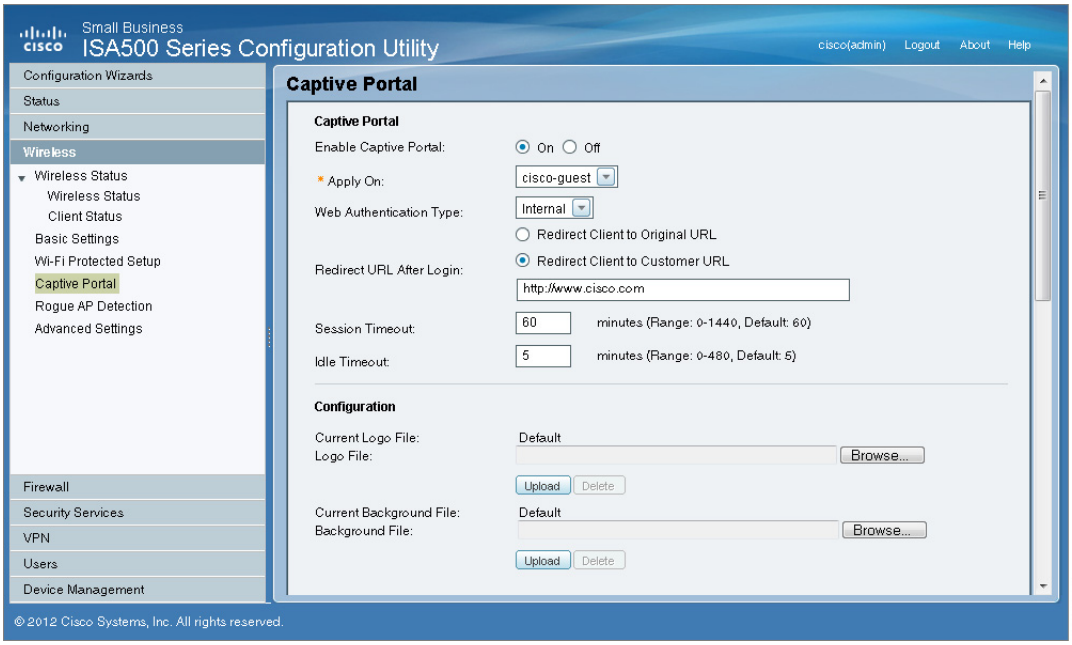
Note: If you chose Internal or External, you will need to use the Users > Users and Groups page to create a User Group with Captive Portal service enabled, and to add users to the group.

STEP 4 **Redirected URL After Login:** Choose one of the following options to determine what happens after a user leaves the portal page:

- **Redirect Client to Customer URL:** Directs the users to a particular URL (such as the URL for your company). If you choose this option, enter the desired URL in the field, including http:// or https://.
- **Redirect Client to Original URL:** Directs the users to the URL that they were trying to access originally.

STEP 5 Configure the timeout settings, or keep the default values.

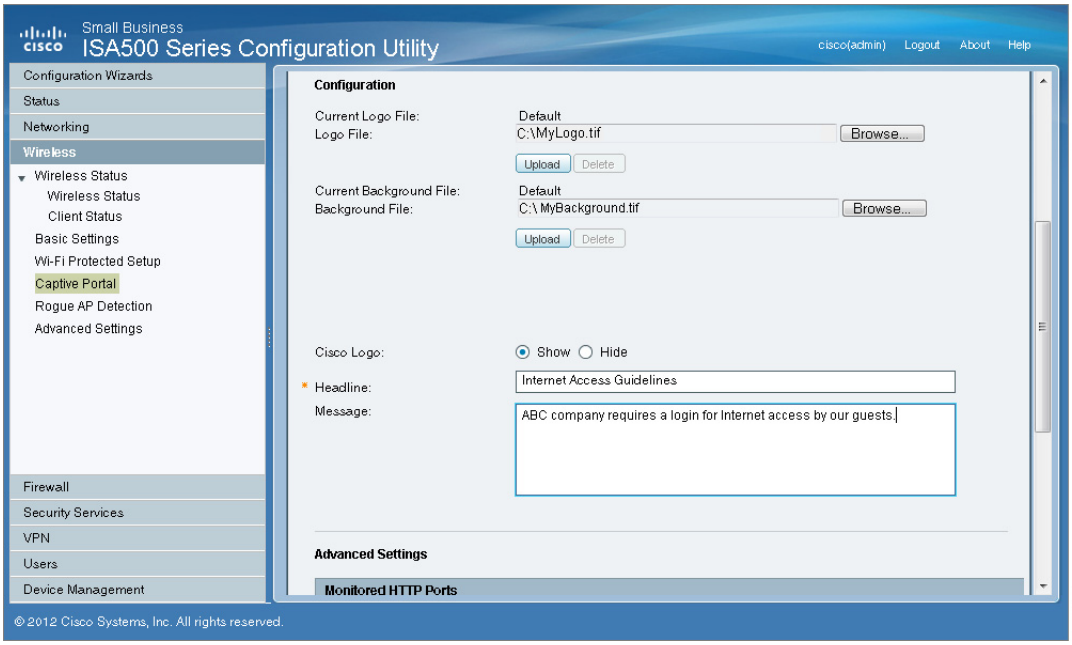
- **Session Timeout:** Enter the maximum number of minutes that a wireless session can remain connected. After the timeout period elapses, the session will be terminated. Enter 0 to allow a user to remain connected without any limit. The default value is 60 minutes.
- **Idle Timeout:** Enter the maximum number of minutes that a wireless session can be idle. After the timeout period elapses, an idle session will be terminated. The default value is 5 minutes.



STEP 6 If you chose **Internal** or **Internal, no auth with accept button**, set up the default HotSpot Login page:

- **Logo File:** You can import an image, such as your corporate logo, to display on the login page. Click **Browse** to locate and select an image file from your local PC and then click **Upload**. To delete the loaded file, click **Delete**.
- **Background File:** You can import an image to display as the background for the login page. Click **Browse** to locate and select an image file (jpg, gif, or png) from your local PC and then click **Upload**. To delete the loaded file, click **Delete**.

  NOTE: When uploading a file, select a bmp, jpg, gif, or png file of 200KB or less. The Current Logo File field displays the filename of the file that is in use, or *Default* if no file has been uploaded for this purpose.
- **Cisco Logo:** If you want to hide the Cisco logo that appears on the login page, choose **Hide**. Otherwise, choose **Show**.
- **Headline:** If you want to create your own headline on the login page, enter the desired text in this field.
- **Message:** If you want to create your own message on the login page, enter the desired text in this field.



STEP 7 If you chose **External** or **External, no auth with accept button**, specify these settings for your external portal page:

- **Authentication Web Server:** Enter the full URL of the external web server (including https://), for example https://172.24.10.10/cgi-bin/PortalLogin.cgi.
- **Authentication Web Key:** Enter the key used to protect the username and password that the external web server sends to the security appliance for authentication.

STEP 8 If you want to use the portal for HTTP requests through other ports besides the default 80 and 443, add the ports in the **Advanced Settings > Monitored HTTP Ports** area.

NOTE: Captive Portal only monitors HTTPS requests through the port 443.

a. Click **Add**.

b. Enter the port number in the **Port** field.

c. Click **OK** to save your settings.

STEP 9 If you want to bypass the portal for certain IP addresses, add them in the **Advanced Settings > Open Domains** area.

a. Click **Add**.

b. Enter the IP address or domain name in the **Domain** field.

c. Click **OK** to save your settings.

STEP 10 Click **Save** to apply your settings.

Troubleshooting

Problem 1: User is not redirected to portal page when internal web authentication type is chosen.

Solution: Either of the following could resolve the problem:

- Check the device is connected to Captive Portals wireless network and the IP address is assigned to the device.
- Check Web Authentication Type is selected as Internal or Internal, no auth with accept button.
- Check the TCP ports on which HTTP requests are sent are added under Monitored HTTP Ports under Advanced Settings on Captive Portal page.

Problem 2: User is not redirected to portal page when internal web authentication type is chosen.

Solution: Either of the following could resolve the problem:

- Check the device is connected to Captive Portals wireless network and the IP address is assigned to the device. .
- Check Web Authentication Type is selected as External or External, no auth with accept button.
- Check the TCP ports on which HTTP requests are sent are added under Monitored HTTP Ports under Advanced Settings on Captive Portal page.
- Check the connectivity of Web-server from ISA500.
- Web-server should be able to accessed by the devices on the Captive Portal wireless network. In other words, the firewall rules associated with

the VLAN to which Captive Portal users join should be able to access the web-server.

- Check if the web-server has any issues.

Using External Web-Hosted CGI Scripts

Following is a CGI script which asks for the authentication information of a user.

The secret string programmed in the **uamsecret** variable should be configured as Authentication Web Key on the Captive portal page. Replace the **MySMB** string in the following section with your company name.

```
# !/usr/bin/perl
# chilli - ChilliSpot.org. A Wireless LAN Access Point Controller
# Copyright (C) 2003, 2004 Mondru AB.
#
# The contents of this file may be used under the terms of the GNU
# General Public License Version 2, provided that the above copyright
# notice and this permission notice is included in all copies or
# substantial portions of the software.

# Redirects from ChilliSpot daemon:
#
# Redirection when not yet or already authenticated
#   notyet:  ChilliSpot daemon redirects to login page.
#   already: ChilliSpot daemon redirects to success status page.
#
# Response to login:
#   already: Attempt to login when already logged in.
#   failed:  Login failed
#   success: Login succeded
#
# logoff:  Response to a logout


# Shared secret used to encrypt challenge with. Prevents dictionary attacks.
# You should change this to your own shared secret.
$uamsecret = "ht2eb8ej6s4et3rg1ulp";

# Uncomment the following line if you want to use ordinary user-password
# for radius authentication. Must be used together with $uamsecret.
$userpassword=1; [1]

# Our own path
$loginpath = $ENV{'SCRIPT_URL'};

use Digest::MD5  qw(md5 md5_hex md5_base64);

# Make sure that the form parameters are clean
```

```
$OK_CHARS='-a-zA-Z0-9_.@&=%!';
$| = 1;
if ($ENV{'CONTENT_LENGTH'}) {
    read (STDIN, $_, $ENV{'CONTENT_LENGTH'});
}
s/[^$OK_CHARS]/_/go;
$input = $_;


# Make sure that the get query parameters are clean
$OK_CHARS='-a-zA-Z0-9_.@&=%!';
$_ = $query=$ENV{QUERY_STRING};
s/[^$OK_CHARS]/_/go;
$query = $_;


# If she did not use https tell her that it was wrong.
if (!($ENV{HTTPS} =~ /^on$/)) {
    print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login Failed</title>[7.1]
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
</head>
<body bgColor = '#c0d8f4'>
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>[7.2]
  <center>
    Login must use encrypted connection.
  </center>
</body>
<!--
<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<WISPAccessGatewayParam
  xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
  xsi:noNamespaceSchemaLocation=
\"http://www.acmewisp.com/WISPAccessGatewayParam.xsd\">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>102</ResponseCode>
<ReplyMessage>Login must use encrypted connection</ReplyMessage>[7.3]
</AuthenticationReply>
</WISPAccessGatewayParam>
-->
</html>
";
    exit(0);
}


#Read form parameters which we care about
@array = split('&',$input);
foreach $var ( @array )
{
```

```
    @array2 = split('=',$var);
    if ($array2[0] =~ /^UserName$/) { $username = $array2[1]; }
    if ($array2[0] =~ /^Password$/) { $password = $array2[1]; }
    if ($array2[0] =~ /^challenge$/) { $challenge = $array2[1]; }
    if ($array2[0] =~ /^button$/) { $button = $array2[1]; }
    if ($array2[0] =~ /^logout$/) { $logout = $array2[1]; }
    if ($array2[0] =~ /^prelogin$/) { $prelogin = $array2[1]; }
    if ($array2[0] =~ /^res$/) { $res = $array2[1]; }
    if ($array2[0] =~ /^uamip$/) { $uamip = $array2[1]; }
    if ($array2[0] =~ /^uamport$/) { $uamport = $array2[1]; }
    if ($array2[0] =~ /^userurl$/)   { $userurl = $array2[1]; }
    if ($array2[0] =~ /^timeleft$/)  { $timeleft = $array2[1]; }
    if ($array2[0] =~ /^redirurl$/)  { $redirurl = $array2[1]; }
}

#Read query parameters which we care about
@array = split('&',$query);
foreach $var ( @array )
{
    @array2 = split('=',$var);
    if ($array2[0] =~ /^res$/)       { $res = $array2[1]; }
    if ($array2[0] =~ /^challenge$/) { $challenge = $array2[1]; }
    if ($array2[0] =~ /^uamip$/)     { $uamip = $array2[1]; }
    if ($array2[0] =~ /^uamport$/)   { $uamport = $array2[1]; }
    if ($array2[0] =~ /^reply$/)     { $reply = $array2[1]; }
    if ($array2[0] =~ /^userurl$/)   { $userurl = $array2[1]; }
    if ($array2[0] =~ /^timeleft$/)  { $timeleft = $array2[1]; }
    if ($array2[0] =~ /^redirurl$/)  { $redirurl = $array2[1]; }
}


$reply =~ s/\+/ /g;
$reply =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$userurldecode = $userurl;
$userurldecode =~ s/\+/ /g;
$userurldecode =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$redirurldecode = $redirurl;
$redirurldecode =~ s/\+/ /g;
$redirurldecode =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$password =~ s/\+/ /g;
$password =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

# If attempt to login
if ($button =~ /^Login$/) {
    $hexchal  = pack "H32", $challenge;
    if (defined $uamsecret) {
   $newchal  = md5($hexchal, $uamsecret);
    }
    else {
   $newchal  = $hexchal;
    }
    $response = md5_hex("\0", $password, $newchal);
```

```
    $pappassword = unpack "H32", ($password ^ $newchal);
#sleep 5;
print "Content-type: text/html\n\n";
print "<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">";
    if ((defined $uamsecret) && defined($userpassword)) {
   print "  <meta http-equiv=\"refresh\" content=\"0;url=
http://$uamip:$uamport/logon?username=$username&password=
$pappassword&userurl=$userurl\">";
    } else {
   print "  <meta http-equiv=\"refresh\" content=\"0;url=
http://$uamip:$uamport/logon?username=$username&response=$response&userurl=
$userurl\">";
    }
print "</head>
<body bgColor = '#c0d8f4'>";
  print "<h1 style=\"text-align: center;\">Logging in to MySMB</h1>";
  print "
  <center>
    Please wait......
  </center>
</body>
<!--
<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<WISPAccessGatewayParam
  xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
  xsi:noNamespaceSchemaLocation=
\"http://www.acmewisp.com/WISPAccessGatewayParam.xsd\">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>201</ResponseCode>
";
    if ((defined $uamsecret) && defined($userpassword)) {
   print "<LoginResultsURL>http://$uamip:$uamport/logon?username=
$username&password=$pappassword</LoginResultsURL>";
    } else {
   print "<LoginResultsURL>http://$uamip:$uamport/logon?username=
$username&response=$response&userurl=$userurl</LoginResultsURL>";
    }
print "</AuthenticationReply>
</WISPAccessGatewayParam>
-->
</html>
";
    exit(0);
}


# Default: It was not a form request
$result = 0;
```

```
# If login successful
if ($res =~ /^success$/) {
    $result = 1;
}

# If login failed
if ($res =~ /^failed$/) {
    $result = 2;
}

# If logout successful
if ($res =~ /^logoff$/) {
    $result = 3;
}

# If tried to login while already logged in
if ($res =~ /^already$/) {
    $result = 4;
}

# If not logged in yet
if ($res =~ /^notyet$/) {
    $result = 5;
}

# If login from smart client
if ($res =~ /^smartclient$/) {
    $result = 6;
}

# If requested a logging in pop up window
if ($res =~ /^popup1$/) {
    $result = 11;
}

# If requested a success pop up window
if ($res =~ /^popup2$/) {
    $result = 12;
}

# If requested a logout pop up window
if ($res =~ /^popup3$/) {
    $result = 13;
}


# Otherwise it was not a form request
# Send out an error message
if ($result == 0) {
    print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login Failed</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
```

```
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
</head>
<body bgColor = '#c0d8f4'>
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>
  <center>
    Login must be performed through MySMB daemon.
  </center>
</body>
</html>
";
    exit(0);
}

#Generate the output
print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login</title>[2.1]
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
  <SCRIPT LANGUAGE=\"JavaScript\">
    var blur = 0;
    var starttime = new Date();
    var startclock = starttime.getTime();
    var mytimeleft = 0;

    function doTime() {
      window.setTimeout( \"doTime()\", 1000 );
      t = new Date();
      time = Math.round((t.getTime() - starttime.getTime())/1000);
      if (mytimeleft) {
        time = mytimeleft - time;
        if (time <= 0) {
          window.location = \"$loginpath?res=popup3&uamip=$uamip&uamport=
$uamport\";
        }
      }
      if (time < 0) time = 0;
      hours = (time - (time % 3600)) / 3600;
      time = time - (hours * 3600);
      mins = (time - (time % 60)) / 60;
      secs = time - (mins * 60);
      if (hours < 10) hours = \"0\" + hours;
      if (mins < 10) mins = \"0\" + mins;
      if (secs < 10) secs = \"0\" + secs;
      title = \"Online time: \" + hours + \":\" + mins + \":\" + secs;
      if (mytimeleft) {
        title = \"Remaining time: \" + hours + \":\" + mins + \":\" + secs;
      }
      if(document.all || document.getElementById){
         document.title = title;
      }
      else {
        self.status = title;
```

```
      }
    }

    function popUp(URL) {
      if (self.name != \"chillispot_popup\") {
        chillispot_popup = window.open(URL, 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
500,height=375');
      }
    }

    function doOnLoad(result, URL, userurl, redirurl, timeleft) {
      if (timeleft) {
        mytimeleft = timeleft;
      }
      if ((result == 1) && (self.name == \"chillispot_popup\")) {
        doTime();
      }
      if ((result == 1) && (self.name != \"chillispot_popup\")) {
        chillispot_popup = window.open(URL, 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
500,height=375');
      }
      if ((result == 2) || result == 5) {
        document.form1.UserName.focus()
      }
      if ((result == 2) && (self.name != \"chillispot_popup\")) {
        chillispot_popup = window.open('', 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
400,height=200');
        chillispot_popup.close();
      }
      if ((result == 12) && (self.name == \"chillispot_popup\")) {
        doTime();
        if (redirurl) {
          opener.location = redirurl;
        }
        else if (userurl) {
          opener.location = userurl;
        }
        else if (opener.home) {
          opener.home();
        }
        else {
          opener.location = \"about:home\";
        }
        self.focus();
        blur = 0;
      }
      if ((result == 13) && (self.name == \"chillispot_popup\")) {
        self.focus();
        blur = 1;
      }
    }
```

```
    function doOnBlur(result) {
      if ((result == 12) && (self.name == \"chillispot_popup\")) {
        if (blur == 0) {
          blur = 1;
          self.focus();
        }
      }
    }
  </script>
</head>
<body onLoad=\"javascript:doOnLoad($result, '$loginpath?res=popup2&uamip=
$uamip&uamport=$uamport&userurl=$userurl&redirurl=$redirurl&timeleft=
$timeleft','$userurldecode', '$redirurldecode', '$timeleft')\" onBlur =
\"javascript:doOnBlur($result)\" bgColor = '#c0d8f4'>";


#      if (!window.opener) {
#        document.bgColor = '#c0d8f4';
#      }

#print "THE INPUT: $input";
#foreach $key (sort (keys %ENV)) {
#  print $key, ' = ', $ENV{$key}, "<br>\n";
#}

if ($result == 2) {
    print "
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>";[6.1]
    if ($reply) {
   print "<center> $reply </BR></BR></center>";
    }
}

if ($result == 5) {
    print "
  <h1 style=\"text-align: center;\">MySMB Login</h1>";[2.2]
}

if ($result == 2 || $result == 5) {
  print "
  <form name=\"form1\" method=\"post\" action=\"$loginpath\">
  <INPUT TYPE=\"hidden\" NAME=\"challenge\" VALUE=\"$challenge\">
  <INPUT TYPE=\"hidden\" NAME=\"uamip\" VALUE=\"$uamip\">
  <INPUT TYPE=\"hidden\" NAME=\"uamport\" VALUE=\"$uamport\">
  <INPUT TYPE=\"hidden\" NAME=\"userurl\" VALUE=\"$userurldecode\">
  <center>
  <table border=\"0\" cellpadding=\"5\" cellspacing=\"0\" style=\"width:
217px;\">
    <tbody>
      <tr>
        <td align=\"right\">Username:</td>[2.3]
        <td><input STYLE=\"font-family: Arial\" type=\"text\" name=
\"UserName\" size=\"20\" maxlength=\"128\"></td>
      </tr>
      <tr>
```

```
        <td align=\"right\">Password:</td>[2.4]
        <td><input STYLE=\"font-family: Arial\" type=\"password\" name=
\"Password\" size=\"20\" maxlength=\"128\"></td>
      </tr>
      <tr>
        <td align=\"center\" colspan=\"2\" height=\"23\"><input type=
\"submit\" name=\"button\" value=\"Login\"[2.5] onClick=
\"javascript:popUp('$loginpath?res=popup1&uamip=$uamip&uamport=
$uamport')\"></td>
      </tr>
    </tbody>
  </table>
  </center>
  </form>
</body>
</html>";
}

if ($result == 1) {
  print "
  <h1 style=\"text-align: center;\">Logged in to MySMB</h1>";[8.1]

  if ($reply) {
      print "<center> $reply </BR></BR></center>";
  }

  print "
  <center>
    <a href=\"http://$uamip:$uamport/logoff\">Logout</a>[8.2]
  </center>
</body>
</html>";
}

if (($result == 4) || ($result == 12)) {
  print "
  <h1 style=\"text-align: center;\">Logged in to MySMB</h1>[4.1]
  <center>
    <a href=\"http://$uamip:$uamport/logoff\">Logout</a>[4.2]
  </center>
</body>
</html>";
}


if ($result == 11) {
  print "<h1 style=\"text-align: center;\">Logging in to MySMB</h1>[3.1]";
  print "
  <center>
    Please wait..... [3.2]
  </center>
</body>
</html>";
}
```

```
if (($result == 3) || ($result == 13)) {
    print "
  <h1 style=\"text-align: center;\">Logged out from MySMB</h1>[5.1]
  <center>
    <a href=\"http://$uamip:$uamport/prelogin\">Login</a>[5.2]
  </center>
</body>
</html>";
}


exit(0);
```

CGI Source Code Example: No Authentication and Accept Button

Following is a CGI script which presents a Accept button on the portal page.

The secret string programmed in **`uamsecret`** variable should be configured as Authentication Web Key on the Captive portal page. Replace the **MySMB** string in the following section with your company name.

```
#!/usr/bin/perl

# chilli - ChilliSpot.org. A Wireless LAN Access Point Controller
# Copyright (C) 2003, 2004 Mondru AB.
#
# The contents of this file may be used under the terms of the GNU
# General Public License Version 2, provided that the above copyright
# notice and this permission notice is included in all copies or
# substantial portions of the software.

# Redirects from ChilliSpot daemon:
#
# Redirection when not yet or already authenticated
#   notyet:  ChilliSpot daemon redirects to login page.
#   already: ChilliSpot daemon redirects to success status page.
#
# Response to login:
#   already: Attempt to login when already logged in.
#   failed:  Login failed
#   success: Login succeded
#
# logoff:  Response to a logout


# Shared secret used to encrypt challenge with. Prevents dictionary attacks.
# You should change this to your own shared secret.
#$uamsecret = "ht2eb8ej6s4et3rg1ulp";
```

```
$uamsecret = "gemteksmb";

# Uncomment the following line if you want to use ordinary user-password
# for radius authentication. Must be used together with $uamsecret.
$userpassword=1;

# Our own path
$loginpath = $ENV{'SCRIPT_URL'};

use Digest::MD5  qw(md5 md5_hex md5_base64);

# Make sure that the form parameters are clean
$OK_CHARS='-a-zA-Z0-9_.@&=%!';
$| = 1;
if ($ENV{'CONTENT_LENGTH'}) {
    read (STDIN, $_, $ENV{'CONTENT_LENGTH'});
}
s/[^$OK_CHARS]/_/go;
$input = $_;


# Make sure that the get query parameters are clean
$OK_CHARS='-a-zA-Z0-9_.@&=%!';
$_ = $query=$ENV{QUERY_STRING};
s/[^$OK_CHARS]/_/go;
$query = $_;


# If she did not use https tell her that it was wrong.
if (!($ENV{HTTPS} =~ /^on$/)) {
    print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login Failed</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
</head>
<body bgColor = '#c0d8f4'>
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>
  <center>
    Login must use encrypted connection.
  </center>
</body>
<!--
<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<WISPAccessGatewayParam
  xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
  xsi:noNamespaceSchemaLocation=
\"http://www.acmewisp.com/WISPAccessGatewayParam.xsd\">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>102</ResponseCode>
<ReplyMessage>Login must use encrypted connection</ReplyMessage>
</AuthenticationReply>
```

```
</WISPAccessGatewayParam>
-->
</html>
";
    exit(0);
}


#Read form parameters which we care about
@array = split('&',$input);
foreach $var ( @array )
{
    @array2 = split('=',$var);
    if ($array2[0] =~ /^UserName$/) { $username = $array2[1]; }
    if ($array2[0] =~ /^Password$/) { $password = $array2[1]; }
    if ($array2[0] =~ /^challenge$/) { $challenge = $array2[1]; }
    if ($array2[0] =~ /^button$/) { $button = $array2[1]; }
    if ($array2[0] =~ /^logout$/) { $logout = $array2[1]; }
    if ($array2[0] =~ /^prelogin$/) { $prelogin = $array2[1]; }
    if ($array2[0] =~ /^res$/) { $res = $array2[1]; }
    if ($array2[0] =~ /^uamip$/) { $uamip = $array2[1]; }
    if ($array2[0] =~ /^uamport$/) { $uamport = $array2[1]; }
    if ($array2[0] =~ /^userurl$/)   { $userurl = $array2[1]; }
    if ($array2[0] =~ /^timeleft$/)  { $timeleft = $array2[1]; }
    if ($array2[0] =~ /^redirurl$/)  { $redirurl = $array2[1]; }
}

#Read query parameters which we care about
@array = split('&',$query);
foreach $var ( @array )
{
    @array2 = split('=',$var);
    if ($array2[0] =~ /^res$/)       { $res = $array2[1]; }
    if ($array2[0] =~ /^challenge$/) { $challenge = $array2[1]; }
    if ($array2[0] =~ /^uamip$/)     { $uamip = $array2[1]; }
    if ($array2[0] =~ /^uamport$/)   { $uamport = $array2[1]; }
    if ($array2[0] =~ /^reply$/)     { $reply = $array2[1]; }
    if ($array2[0] =~ /^userurl$/)   { $userurl = $array2[1]; }
    if ($array2[0] =~ /^timeleft$/)  { $timeleft = $array2[1]; }
    if ($array2[0] =~ /^redirurl$/)  { $redirurl = $array2[1]; }
}


$reply =~ s/\+/ /g;
$reply =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$userurldecode = $userurl;
$userurldecode =~ s/\+/ /g;
$userurldecode =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$redirurldecode = $redirurl;
$redirurldecode =~ s/\+/ /g;
$redirurldecode =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$password =~ s/\+/ /g;
```

```
$password =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

# If attempt to login
if ($button =~ /^Accept$/) {
    $hexchal  = pack "H32", $challenge;
    if (defined $uamsecret) {
   $newchal  = md5($hexchal, $uamsecret);
    }
    else {
   $newchal  = $hexchal;
    }
    $response = md5_hex("\0", $password, $newchal);
    $pappassword = unpack "H32", ($password ^ $newchal);
#sleep 5;
print "Content-type: text/html\n\n";
print "<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">";
    if ((defined $uamsecret) && defined($userpassword)) {
   print "  <meta http-equiv=\"refresh\" content=\"0;url=
http://$uamip:$uamport/logon?username=$username&password=
$pappassword&userurl=$userurl\">";
    } else {
   print "  <meta http-equiv=\"refresh\" content=\"0;url=
http://$uamip:$uamport/logon?username=$username&response=$response&userurl=
$userurl\">";
    }
print "</head>
<body bgColor = '#c0d8f4'>";
  print "<h1 style=\"text-align: center;\">Logging in to MySMB</h1>";
  print "
  <center>
    Please wait......
  </center>
</body>
<!--
<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<WISPAccessGatewayParam
  xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
  xsi:noNamespaceSchemaLocation=
\"http://www.acmewisp.com/WISPAccessGatewayParam.xsd\">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>201</ResponseCode>
";
    if ((defined $uamsecret) && defined($userpassword)) {
   print "<LoginResultsURL>http://$uamip:$uamport/logon?username=
$username&password=$pappassword</LoginResultsURL>";
    } else {
   print "<LoginResultsURL>http://$uamip:$uamport/logon?username=
$username&response=$response&userurl=$userurl</LoginResultsURL>";
    }
```

```
print "</AuthenticationReply>
</WISPAccessGatewayParam>
-->
</html>
";
    exit(0);
}


# Default: It was not a form request
$result = 0;

# If login successful
if ($res =~ /^success$/) {
    $result = 1;
}

# If login failed
if ($res =~ /^failed$/) {
    $result = 2;
}

# If logout successful
if ($res =~ /^logoff$/) {
    $result = 3;
}

# If tried to login while already logged in
if ($res =~ /^already$/) {
    $result = 4;
}

# If not logged in yet
if ($res =~ /^notyet$/) {
    $result = 5;
}

# If login from smart client
if ($res =~ /^smartclient$/) {
    $result = 6;
}

# If requested a logging in pop up window
if ($res =~ /^popup1$/) {
    $result = 11;
}

# If requested a success pop up window
if ($res =~ /^popup2$/) {
    $result = 12;
}

# If requested a logout pop up window
if ($res =~ /^popup3$/) {
    $result = 13;
```

```
}


# Otherwise it was not a form request
# Send out an error message
if ($result == 0) {
    print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login Failed</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
</head>
<body bgColor = '#c0d8f4'>
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>
  <center>
    Login must be performed through MySMB daemon.
  </center>
</body>
</html>
";
    exit(0);
}

#Generate the output
print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
  <SCRIPT LANGUAGE=\"JavaScript\">
    var blur = 0;
    var starttime = new Date();
    var startclock = starttime.getTime();
    var mytimeleft = 0;

    function doTime() {
      window.setTimeout( \"doTime()\", 1000 );
      t = new Date();
      time = Math.round((t.getTime() - starttime.getTime())/1000);
      if (mytimeleft) {
        time = mytimeleft - time;
        if (time <= 0) {
          window.location = \"$loginpath?res=popup3&uamip=$uamip&uamport=
$uamport\";
        }
      }
      if (time < 0) time = 0;
      hours = (time - (time % 3600)) / 3600;
      time = time - (hours * 3600);
      mins = (time - (time % 60)) / 60;
      secs = time - (mins * 60);
```

```
      if (hours < 10) hours = \"0\" + hours;
      if (mins < 10) mins = \"0\" + mins;
      if (secs < 10) secs = \"0\" + secs;
      title = \"Online time: \" + hours + \":\" + mins + \":\" + secs;
      if (mytimeleft) {
        title = \"Remaining time: \" + hours + \":\" + mins + \":\" + secs;
      }
      if(document.all || document.getElementById){
         document.title = title;
      }
      else {
        self.status = title;
      }
    }

    function popUp(URL) {
      if (self.name != \"chillispot_popup\") {
        chillispot_popup = window.open(URL, 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
500,height=375');
      }
    }

    function doOnLoad(result, URL, userurl, redirurl, timeleft) {
   if (timeleft) {
        mytimeleft = timeleft;
      }
      if ((result == 1) && (self.name == \"chillispot_popup\")) {
        doTime();
      }
      if ((result == 1) && (self.name != \"chillispot_popup\")) {
        chillispot_popup = window.open(URL, 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
500,height=375');
      }
      if ((result == 2) || result == 5) {
        //document.form1.UserName.focus()
      }
      if ((result == 2) && (self.name != \"chillispot_popup\")) {
        chillispot_popup = window.open('', 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
400,height=200');
        chillispot_popup.close();
      }
      if ((result == 12) && (self.name == \"chillispot_popup\")) {
        doTime();
        if (redirurl) {
          opener.location = redirurl;
        }
        else if (userurl) {
          opener.location = userurl;
        }
        else if (opener.home) {
          opener.home();
        }
```

```
        else {
          opener.location = \"about:home\";
        }
        self.focus();
        blur = 0;
      }
      if ((result == 13) && (self.name == \"chillispot_popup\")) {
        self.focus();
        blur = 1;
      }
    }

    function doOnBlur(result) {
      if ((result == 12) && (self.name == \"chillispot_popup\")) {
        if (blur == 0) {
          blur = 1;
          self.focus();
        }
      }
    }
  </script>
</head>
<body onLoad=\"javascript:doOnLoad($result, '$loginpath?res=popup2&uamip=
$uamip&uamport=$uamport&userurl=$userurl&redirurl=$redirurl&timeleft=
$timeleft','$userurldecode', '$redirurldecode', '$timeleft')\" onBlur =
\"javascript:doOnBlur($result)\" bgColor = '#c0d8f4'>";


#      if (!window.opener) {
#        document.bgColor = '#c0d8f4';
#      }

#print "THE INPUT: $input";
#foreach $key (sort (keys %ENV)) {
#  print $key, ' = ', $ENV{$key}, "<br>\n";
#}

if ($result == 2) {
    print "
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>";
    if ($reply) {
    print "<center> $reply </BR></BR></center>";
    }
}

if ($result == 5) {
    print "
  <h1 style=\"text-align: center;\">MySMB Login</h1>";
}

if ($result == 2 || $result == 5) {
  print "
  <form name=\"form1\" method=\"post\" action=\"$loginpath\">
  <INPUT TYPE=\"hidden\" NAME=\"challenge\" VALUE=\"$challenge\">
  <INPUT TYPE=\"hidden\" NAME=\"uamip\" VALUE=\"$uamip\">
```

```
  <INPUT TYPE=\"hidden\" NAME=\"uamport\" VALUE=\"$uamport\">
  <INPUT TYPE=\"hidden\" NAME=\"userurl\" VALUE=\"$userurldecode\">
  <INPUT TYPE=\"hidden\" NAME=\"UserName\" VALUE=\"\">
  <INPUT TYPE=\"hidden\" NAME=\"Password\" VALUE=\"\">
  <center>
  <table border=\"0\" cellpadding=\"5\" cellspacing=\"0\" style=\"width:
217px;\">
    <tbody>
      <tr>
        <td align=\"center\" colspan=\"2\" height=\"23\"><input type=
\"submit\" name=\"button\" value=\"Accept\" onClick=
\"javascript:popUp('$loginpath?res=popup1&uamip=$uamip&uamport=
$uamport')\"></td>
      </tr>
    </tbody>
  </table>
  </center>
  </form>
</body>
</html>";
}

if ($result == 1) {
  print "
  <h1 style=\"text-align: center;\">Logged in to MySMB</h1>";

  if ($reply) {
      print "<center> $reply </BR></BR></center>";
  }

  print "
  <center>
    <a href=\"http://$uamip:$uamport/logoff\">Logout</a>
  </center>
</body>
</html>";
}

if (($result == 4) || ($result == 12)) {
  print "
  <h1 style=\"text-align: center;\">Logged in to MySMB</h1>
  <center>
    <a href=\"http://$uamip:$uamport/logoff\">Logout</a>
  </center>
</body>
</html>";
}


if ($result == 11) {
  print "<h1 style=\"text-align: center;\">Logging in to MySMB</h1>";
  print "
  <center>
    Please wait......
  </center>
```

```
</body>
</html>";
}


if (($result == 3) || ($result == 13)) {
    print "
  <h1 style=\"text-align: center;\">Logged out from MySMB</h1>
  <center>
    <a href=\"http://$uamip:$uamport/prelogin\">Login</a>
  </center>
</body>
</html>";
}


exit(0);
```

Related Information

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Cisco Small Business Firmware Downloads	www.cisco.com/go/isa500software
Cisco Small Business Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Documentation	
Product Documentation	www.cisco.com/go/isa500resources
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb

Cisco Small Business Home	www.cisco.com/smb

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.

78-21182-01

5

Wireless (for ISA550W and ISA570W only)

This chapter describes how to configure your wireless network. It includes the following sections:

- Viewing Wireless Status, page 207
- Configuring the Basic Settings, page 208
- Configuring SSID Profiles, page 210
- Configuring Wi-Fi Protected Setup, page 219
- Configuring Captive Portal, page 221
- Configuring Wireless Rogue AP Detection, page 247
- Advanced Radio Settings, page 248

To access the Wireless pages, click **Wireless** in the left hand navigation pane.

Viewing Wireless Status

This section describes how to view information for your wireless network. Refer to the following topics:

- Viewing Wireless Statistics, page 207
- Viewing Wireless Client Status, page 208

Viewing Wireless Statistics

Use the Wireless Status page to view the cumulative total of relevant wireless statistics for all SSIDs. This page is automatically updated every 10 seconds. Click Refresh to manually refresh the data.

Wireless > Wireless Status > Wireless Status

Field	Description
Wireless Status	
SSID Number	Number of the SSID.
SSID Name	Name of the SSID.
MAC Address	MAC address of the SSID.
VLAN	VLAN to which the SSID is mapped.
Client List	Number of client stations that are connected to the SSID.
Wireless Statistics	
Name	Name of the SSID.
Tx Packets	Number of transmitted packets on the SSID.
Rx Packets	Number of received packets on the SSID.
Collisions	Number of packet collisions reported to the SSID.
Tx Bytes/Sec	Number of transmitted bytes of information on the SSID.
Rx Bytes/Sec	Number of received bytes of information on the SSID.
Uptime	Time that the SSID has been active.

Viewing Wireless Client Status

Use the Client Status page to view information for all client stations that are already connected to each SSID. The MAC address and IP address for all connected client stations for each SSID are displayed. To open this page, click **Wireless > Wireless Status > Client Status**. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

Configuring the Basic Settings

Use the Basic Settings page to change the wireless mode to suit the devices in your network, specify the wireless channel and bandwidth for operation to resolve issues with interference from other access points in the area, or enable U-APSD and SSID Isolation if needed.

STEP 1 Click **Wireless > Basic Settings**.

STEP 2 Enter the following information:

- **Wireless Radio:** Click **On** to turn wireless radio on and hence enable the SSID called “cisco-data,” or click **Off** to turn wireless radio off. Enabling any SSID will turn on wireless radio. Disabling all SSIDs will turn off wireless radio.
- **Wireless Mode:** Choose the 802.11 modulation technique.
  - **802.11b/g mixed:** Choose this mode if some devices in the wireless network use 802.11b and others use 802.11g. Both 802.11b and 802.11g clients can connect to the access point.
  - **802.11b/g/n mixed:** Choose this mode to allow 802.11b, 802.11g, and 802.11n clients operating in the 2.4 GHz frequency to connect to the access point.
  - **802.11n only:** Choose this mode if all devices in the wireless network can support 802.11n. Only 802.11n clients operating in the 2.4 GHz frequency can connect to the access point.
- **Wireless Channel:** Choose a channel from a list of channels or choose **Auto** to let the system determine the optimal channel to use based on the environmental noise levels for the available channels.

- **Bandwidth Channel:** Choose 20 MHz channel bonding (spacing), or choose **Auto** to let the system determine the optimal channel spacing to use. This setting is specific to 802.11n traffic.
- **Extension Channel:** Choose either Lower or Upper if you choose Auto channel spacing.
- **Unscheduled Automatic Power Save Delivery (U-APSD):** Click **Enable** to enable U-APSD to conserve the power, or click **Disable** to disable it.
- **SSID Isolation:** Click **Enable** to enable the SSID Isolation feature so that the SSIDs will be unable to see each other when the SSIDs belong to the same VLAN, or click **Disable** to disable it. When you enable SSID Isolation (among the SSIDs), traffic on one SSID will not be forwarded to any other SSID.

STEP 3 In the **SSIDs** area, all predefined SSIDs on the security appliance appear in the table. You can configure the following properties for each predefined SSID:

- **Enable:** Check this box to enable a SSID, uncheck this box to disable a SSID. By default, all SSIDs are disabled.
- **SSID Name:** Enter the name for a SSID.
- **SSID Broadcast:** Check this box to broadcast the SSID in its beacon frames. All wireless devices within range are able to see the SSID when they scan for available networks. Uncheck this box to prevent auto-detection of the SSID. In this case, users must know the SSID to set up a wireless connection to this SSID.

  NOTE: Disabling SSID Broadcast is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect or monitor unencrypted traffic. Suppressing the SSID broadcast offers a very minimal level of protection on an otherwise exposed network (such as a guest network) where the priority is making it easy for clients to get a connection and where no sensitive information is available.
- **Security Mode:** Displays the security mode currently used for the SSID. To configure the security settings for the SSID, click the **Edit** (pencil) icon. See **Configuring Wireless Security, page 211**.
- **MAC Filtering:** Shows if the MAC Filtering feature is enabled or disabled on the SSID. MAC Filtering can permit or block access to the SSID by the MAC (hardware) address of the requesting device. To configure the MAC Filtering settings for the SSID, click the **Edit** (pencil) icon. See **Controlling Wireless Access Based on MAC Addresses, page 217**.

- **VLAN Mapping:** Displays the VLAN to which the SSID is mapped. All traffic from the wireless clients that are connected to this SSID will be directed to the selected VLAN. To associate the SSID to a specific VLAN, click the **Edit** (pencil) icon. See **Mapping the SSID to VLAN, page 218**.
- **Wi-Fi Multimedia:** Check this box to enable Wi-Fi Multimedia (WMM), which is designed to improve the user experience for audio, video, and voice applications over a Wi-Fi wireless connection. WMM refers to QoS over Wi-Fi. QoS enables Wi-Fi access points to prioritize traffic and optimizes the way shared network resources are allocated among different applications. By default, WMM is enabled when you choose a wireless mode that includes 802.11n.
- **Station Isolation:** Check so that the wireless clients on the same SSID will be unable to see each other.

STEP 4 Click **Save** to apply your settings.

Configuring SSID Profiles

ISA550W and ISA570W support four SSIDs. By default, all SSIDs are disabled. For security purposes, we strongly recommend that you configure each SSID with the highest level of security that is supported by the devices into your wireless network.

Multiple SSIDs can segment the wireless LAN into multiple broadcast domains. This configuration helps you to maintain better control over broadcast and multicast traffic, which affects network performance.

Refer to the following topics:

- **Configuring Wireless Security, page 211**
- **Controlling Wireless Access Based on MAC Addresses, page 217**
- **Mapping the SSID to VLAN, page 218**
- **Configuring SSID Schedule, page 218**

Configuring Wireless Security

This section describes how to configure the security mode for the SSID. All devices on this network must use the same security mode and settings to work correctly. Cisco recommends using the highest level of security that is supported by the devices in your network.

NOTE If the security mode is set as WEP or as WPA with TKIP encryption algorithm for the SSID that supports 802.11n, the transmit rate for its associated client stations will not exceed 54 Mbps.

STEP 1 Click **Wireless > Basic Settings**.

STEP 2 In the **SSIDs** area, click the **Edit** (pencil) icon to edit the settings for the SSID.

The SSID - Edit window opens.

STEP 3 In the **Security Mode** tab, specify the following information:

- **SSID Name:** The name of the SSID on which the security settings are applied.
- **User Limit:** Specify the maximum number of users that can simultaneously connect to this SSID. Enter a value in the range 0 to 200. The value of zero (0) indicates that there is no limit for this SSID.

  NOTE: The maximum number of users that can simultaneously connect to all enabled SSIDs is 200.
- **Security Mode:** Choose the type of security.

Security Mode	Description
Open	Any wireless device that is in range can connect to the SSID. This is the default setting but not recommended.

Security Mode	Description
WEP	Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and SSIDs on the network are configured with a static 64-bit or 128-bit Shared Key for data encryption. The higher the bit for data encryption, the more secure for your network. WEP encryption is an older encryption method that is not considered to be secure and can easily be broken. Choose this option only if you need to allow access to devices that do not support WPA or WPA2.
WPA	Wi-Fi Protected Access (WPA) provides better security than WEP because it uses dynamic key encryption. This standard was implemented as an intermediate measure to replace WEP, pending final completion of the 802.11i standard for WPA2. The security appliance supports the following WPA security modes. Choose one of them if you need to allow access to devices that do not support WPA2. ▪ **WPA-Personal:** Supports TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption System) encryption mechanisms for data encryption (default is TKIP). TKIP uses dynamic keys and incorporates Message Integrity Code (MIC) to provide protection against hackers. AES uses symmetric 128-bit block data encryption. ▪ **WPA-Enterprise:** Uses WPA with RADIUS authentication. This mode supports TKIP and AES encryption mechanisms (default is TKIP) and requires the use of a RADIUS server to authenticate users.

Security Mode	Description
WPA2	WPA2 provides the best security for wireless transmissions. This method implements the security standards specified in the final version of 802.11i. The security appliance supports the following WPA2 security modes: ▪ **WPA2-Personal:** Always uses AES encryption mechanism for data encryption. ▪ **WPA2-Enterprise:** Uses WPA2 with RADIUS authentication. This mode always uses AES encryption mechanism for data encryption and requires the use of a RADIUS server to authenticate users.
WPA + WPA2	Allows both WPA and WPA2 clients to connect simultaneously. The SSID automatically chooses the encryption algorithm used by each client device. This security mode is a good choice to enable a higher level of security while allowing access by devices that might not support WPA2. The security appliance supports the following WPA+WPA2 security modes: ▪ **WPA/WPA2-Personal mixed:** Supports the transition from WPA-Personal to WPA2-Personal. You can have client devices that use either WPA-Personal or WPA2-Personal. ▪ **WPA/WPA2-Enterprise mixed:** Supports the transition from WPA-Enterprise to WPA2-Enterprise. You can have client devices that use either WPA-Enterprise or WPA2-Enterprise.
RADIUS	Uses RADIUS servers for client authentication and dynamic WEP key generation for data encryption.

STEP 4 If you choose **Open** as the security mode, no other options are configurable. This mode means that any data transferred to and from the SSID is not encrypted. This security mode can be useful during initial network configuration or for problem solving, but it is not recommended for regular use on the internal network because it is not secure.

STEP 5 If you choose **WEP** as the security mode, enter the following information:

- **Authentication Type:** Choose either **Open System** or **Shared key**, or choose **Auto** to let the security appliance accept both Open System and Shared Key schemes.
- **Default Transmit Key:** Choose a key index as the default transmit key. Key indexes 1 through 4 are available.
- **Encryption:** Choose the encryption type: 64 bits (10 hex digits), 64 bits (5 ASCII), 128 bits (26 hex digits), or 128 bits (13 ASCII). The default is 64 bits (10 hex digits). The larger size keys provide stronger encryption, thus making the key more difficult to crack.
- **Passphrase:** If you want to generate WEP keys by using a Passphrase, enter any alphanumeric phrase (between 4 to 63 characters) and then click **Generate** to generate 4 unique WEP keys. Select one key to use as the key that devices must have to use the wireless network.
- **Key 1-4:** If a WEP Passphrase is not specified, a key can be entered directly into one of the Key boxes. The length of the key should be 5 ASCII characters (or 10 hex characters) for 64-bit encryption and 13 ASCII characters (or 26 hex characters) for 128-bit encryption.

STEP 6 If you choose **WPA-Personal** as the security mode, enter the following information:

- **Encryption:** Choose either TKIP or TKIP_CCMP (AES) as the encryption algorithm for data encryption. The default is TKIP.
- **Shared Secret:** The Pre-shared Key (PSK) is the shared secret key for WPA. Enter a string of at least 8 characters to a maximum of 63 characters.
- **Key Renewal Timeout:** Enter a value to set the interval at which the key is refreshed for clients associated to this SSID. The valid range is 0 to 4194303 seconds. A value of zero (0) indicates that the key is not refreshed. The default value is 3600 seconds.

STEP 7 If you choose **WPA2-Personal** as the security mode, enter the following information:

- **Encryption:** Always use AES for data encryption.
- **Shared Secret:** The Pre-shared Key (PSK) is the shared secret key for WPA. Enter a string of at least 8 characters to a maximum of 63 characters.

- **Key Renewal Timeout:** Enter a value to set the interval at which the key is refreshed for clients associated to this SSID. The valid range is 0 to 4194303 seconds. A value of zero (0) indicates that the key is not refreshed. The default value is 3600 seconds.

STEP 8 If you choose **WPA/WPA2-Personal mixed** as the security mode, enter the following information:

- **Encryption:** Automatically choose TKIP or AES for data encryption.
- **Shared Secret:** The Pre-shared Key (PSK) is the shared secret key for WPA. Enter a string of at least 8 characters to a maximum of 63 characters.
- **Key Renewal Timeout:** Enter a value to set the interval at which the key is refreshed for clients associated to this SSID. The valid range is 0 to 4194303 seconds. A value of zero (0) indicates that the key is not refreshed. The default value is 3600 seconds.

STEP 9 If you choose **WPA-Enterprise** as the security mode, enter the following information:

- **Encryption:** Choose either TKIP or AES as the encryption algorithm for data encryption. The default is TKIP.
- **Key Renewal Timeout:** Enter a value to set the interval at which the key is refreshed for clients associated to this SSID. The valid range is 0 to 4194303 seconds. A value of zero (0) indicates that the key is not refreshed. The default value is 3600 seconds.
- **RADIUS Server ID:** The security appliance predefines three RADIUS groups. Choose an existing RADIUS group for client authentication. The following RADIUS server settings of the selected group are displayed.
  - **Primary RADIUS Server IP Address:** The IP address of the primary RADIUS server.
  - **Primary RADIUS Server Port:** The port number of the primary RADIUS server.
  - **Primary RADIUS Server Shared Secret:** The shared secret key of the primary RADIUS server.
  - **Secondary RADIUS Server IP Address:** The IP address of the secondary RADIUS server.
  - **Secondary RADIUS Server Port:** The port number of the secondary RADIUS server.

- **Secondary RADIUS Server Shared Secret:** The shared secret key of the secondary RADIUS server.

  NOTE: You can change the settings in the above fields but the RADIUS server settings you specify will replace the default settings of the selected group. To maintain the RADIUS servers, go to the Users > RADIUS Servers page. See Configuring RADIUS Servers, page 401.

STEP 10 If you choose **WPA2-Enterprise** as the security mode, enter the following information:

- **Encryption:** Always use AES encryption algorithm for data encryption.
- **Key Renewal Timeout:** Enter a value to set the interval at which the key is refreshed for clients associated to this SSID. The valid range is 0 to 4194303 seconds. A value of zero (0) indicates that the key is not refreshed. The default value is 3600 seconds.
- **RADIUS Server ID:** Choose an existing RADIUS group for client authentication. The RADIUS server settings of the selected group are displayed. You can change the RADIUS server settings but the settings you specify will replace the default settings of the selected group. To maintain the RADIUS servers, go to the Users > RADIUS Servers page. See Configuring RADIUS Servers, page 401.

STEP 11 If you choose **WPA/WPA2-Enterprise Mixed** as the security mode, enter the following information:

- **Encryption:** Automatically choose TKIP or AES encryption algorithm for data encryption.
- **Key Renewal Timeout:** Enter a value to set the interval at which the key is refreshed for clients associated to this SSID. The valid range is 0 to 4194303 seconds. A value of zero (0) indicates that the key is not refreshed. The default value is 3600 seconds.
- **RADIUS Server ID:** Choose an existing RADIUS group for client authentication. The RADIUS server settings of the selected group are displayed. You can change the RADIUS server settings but the settings you specify will replace the default settings of the selected group. To maintain the RADIUS servers, go to the Users > RADIUS Servers page. See Configuring RADIUS Servers, page 401.

STEP 12 If you choose **RADIUS** as the security mode, choose an existing RADIUS group for client authentication from the **RADIUS Server ID** drop-down list. The RADIUS server settings of the selected group are displayed. You can change the RADIUS server settings but the settings you specify will replace the default settings of the

selected group. To maintain the RADIUS servers, go to the Users > RADIUS Servers page. See Configuring RADIUS Servers, page 401.

STEP 13 Click **OK** to save your settings.

STEP 14 Click **Save** to apply your settings.

Controlling Wireless Access Based on MAC Addresses

MAC Filtering allows or blocks access to the SSID by the MAC (hardware) address of the requesting device. By default, MAC Filtering is disabled for each SSID.

MAC Filtering provides additional security, but it also adds to the complexity and maintenance. You need to specify the list of MAC addresses that you want to block or allow. Be sure to enter each MAC address correctly to ensure that the policy is applied as intended. Generally it is easier and more secure to use this feature to allow access to the specified MAC addresses, thereby denying access to unknown MAC addresses.

STEP 1 Click **Wireless > Basic Settings**.

STEP 2 In the **SSIDs** area, click the **Edit** (pencil) icon to edit the settings for the SSID.

The SSID - Edit window opens.

STEP 3 In the **MAC Filtering** tab, enter the following information:

- **SSID Name:** The name of the SSID on which the MAC Filtering settings are applied.
- **Connection Control:** Choose one of the following options as the MAC Filtering policy:
  - **Disable:** Disable MAC Filtering for the SSID.
  - **Allow only the following MAC addresses to connect to the wireless network:** All devices in list of MAC addresses are allowed to connect to this SSID. All other devices are blocked.
  - **Prevent the following MAC addresses from connecting to the wireless network:** All devices in list of MAC addresses are prevented from connecting to this SSID. All other devices are allowed.

STEP 4 In the **Connection Control List** area, specify the list of MAC addresses that you want to block or allow. You can add up to 16 MAC addresses.

STEP 5 Click **OK** to save your settings.

STEP 6 Click **Save** to apply your settings.

Mapping the SSID to VLAN

STEP 1 Click **Wireless > Basic Settings**.

STEP 2 In the **SSIDs** area, click the **Edit** (pencil) icon to edit the settings for the SSID.

The SSID - Edit window opens.

STEP 3 In the **VLANs** tab, enter the following information:

- **SSID Name:** The name of the SSID to which the VLAN is mapped.
- **VLAN:** Choose the VLAN from the drop-down list. The SSID is mapped to the selected VLAN. All traffic from the wireless clients that are connected to this SSID will be directed to the selected VLAN.

STEP 4 Click **OK** to save your settings.

STEP 5 Click **Save** to apply your settings.

Configuring SSID Schedule

This section describes how to specify the schedule to keep the SSID active within a specific time per day.

STEP 1 Click **Wireless > Basic Settings**.

STEP 2 In the **SSIDs** area, click the **Edit** (pencil) icon to edit the settings for the SSID.

The SSID - Edit window opens.

STEP 3 In the **Scheduling** tab, specify the time per day to keep the SSID active:

- **SSID Name:** The name of the SSID on which the schedule setting is applied.

- **Active Time:** Click **On** to enable the schedule feature for the SSID, or click **Off** to disable it. Disabling the schedule feature will keep the SSID active in 24 hours per day. If you enable this feature, configure the time range per day to keep this SSID active.
  - **Start Time:** Enter the values in the hour and minute fields and choose AM or PM from the drop-down list.
  - **Stop Time:** Enter the values in the hour and minute fields and choose AM or PM from the drop-down list.

STEP 4 Click **OK** to save your settings.

STEP 5 Click **Save** to apply your settings.

Configuring Wi-Fi Protected Setup

Use the Wi-Fi Protected Setup page to configure Wi-Fi Protected Setup (WPS) on the security appliance to allow WPS-enabled devices to more easily connect to the wireless network.

STEP 1 Click **Wireless > Wi-Fi Protected Setup**.

The Wi-Fi Protected Setup window opens.

STEP 2 Click **On** to enable WPS, or click **Off** to disable it.

STEP 3 If you enable WPS, specify the following WPS settings:

- **WPS Configuration Status:** Determines whether to start a new configuration on the SSID before the wireless client establishes a WPS connection.
  - **Configured:** If you choose this option, the wireless clients will associate with the SSID by following the original security settings of the SSID, which may cause an un-secured connection if the SSID is not configured properly in advance, for example the security mode is set to “Open.” To provide a secured connection under the Configured status, you can manually change the security mode for the SSID in advance and then establish the WPS connection.

- **Unconfigured:** If you choose this option, the SSID will automatically configure its security settings such as the SSID name and the security mode before the wireless clients are associated to provide a secured connection. After the wireless clients are connected, the status will be automatically changed to "Configured." Any change for the SSID name, the security mode, or the WEP key or passphrase will change the status to "Configured."

- **Network Name (SSID):** Choose the SSID on which the WPS settings are applied.
- **Security:** The security mode currently used for the selected SSID.
- **Encryption:** The encryption method currently used for the selected SSID.

STEP 4 If the wireless client device has a WPS push button, follow these steps to establish the WPS connection:

a. Enable WPS on the security appliance.

b. Click the **WPS** button on this page.

c. Press the **WPS** push button on the wireless client device within 2 minutes.

d. Verify that the wireless client is connected to the SSID.

STEP 5 If the wireless client device has a WPS PIN number, follow these steps to establish the WPS connection:

a. Get the PIN number used on the wireless client device.

b. Enable WPS on the security appliance.

c. Enter the PIN number in the field and click **Apply** to register the PIN number.

d. Enable WPS on the wireless client device within 2 minutes.

e. Verify that the wireless client is connected to the SSID.

STEP 6 If the wireless client device asks for the PIN number of the security appliance, follow these steps to establish the WPS connection:

a. Enable WPS on the security appliance.

b. Click **Generate** to generate a PIN number.

c. Follow the instructions on the wireless client device to configure WPS within 2 minutes by using the registered PIN number.

d. Verify that the wireless client device is connected to the SSID.

NOTE: If the wireless client device does not connect to the SSID after 2 minutes, please manually disable WPS on the security appliance to prevent the WPS brute-force attack.

STEP 7 Click **Save** to apply your settings.

Configuring Captive Portal

You may want to direct users to a web portal before they can access the Internet through the security appliance. To achieve this goal, you can enable Captive Portal on a wireless network, a VLAN, or a DMZ.

When a user in a Captive Portal user group attempts to access the Internet via a web browser, a portal page appears. You can require a log in or the entry of payment information, for example, and you can set up the portal page to display information, usage guidelines, warning messages, and so on. After successfully logging in, paying, or acknowledging your messages, the user can use other applications on the PC to communicate with the network.

In addition to the portal options mentioned above, additional options make it easy to adapt the Captive Portal feature to your needs:

- You can specify certain domains that users can access without going through the portal.
- The portal page can be stored locally on the ISA500 device or on an external web server that you specify.

Requirements

This feature is compatible with these browsers:

- Internet Explorer (v 8.0 or above)
- Firefox (v 9.0 or above)
- Google Chrome
- Safari

A computer accessing the Captive Portal must have one of these operating systems:

- Windows 7
- Windows XP
- Mac OS

Captive Portal also can be used from a mobile device with one of these operating systems:

- iOS (iPhone, iPad)
- Android

Before You Begin

Before you configure your portal, you may need to configure VLANs, SSIDs, and users. Read the following information to determine what steps may be needed to achieve your goals.

VLAN Setup

No special VLAN configuration is required for a Captive Portal, but you may want to consider the points below before proceeding. To configure VLANs, use the Networking > VLAN page..

- Each SSID is associated with a VLAN. You can use the pre-configured VLANs (DEFAULT, GUEST, and VOICE) or add a custom VLAN.

- You may want to associate a VLAN, such as the GUEST VLAN, with a security zone so that you can configure appropriate security policies. For example, you can apply URL filtering policies to the zone to prevent access to certain types of websites.
- A Captive Portal must be associated either with a single SSID or with a VLAN. If you want to enable a portal for users of multiple SSIDs, you will need to assign them all to the same VLAN. You can use a pre-configured VLAN or can create a VLAN for this purpose.

Wireless Setup

For a Captive Portal on the wireless network, you must enable the wireless radio and at least one SSID before you can enable a Captive Portal. To configure these settings, use the Wireless > Basic Settings page. .

- Enable the wireless radio.
- Enable the SSID(s) that you want to use for the portal.
- If you created a special VLAN for use with your Captive Portal, assign it to the SSID(s) that you want to use for the portal.

User Authentication

If you want to require user authentication for your portal, the security appliance can authenticate the users by using the local database and an external AAA server (such as RADIUS, AD, and LDAP). The authentication method is derived from the user authentication settings that you specified in the Users > User Authentication page. See Configuring User Authentication Settings, page 393.

For the local database option, you need to set up a User Group with the Captive Portal service enabled, and add the users' names and passwords. .

Configuring a Captive Portal

You configure this feature separately for the wireless network (**Wireless > Captive Portal**) and for the wired network (**Networking > Captive Portal**).

STEP 1 **Enable Captive Portal:** Click **On** to enable the Captive Portal feature.

STEP 2 **Apply On:** Choose the SSID, VLAN, or DMZ interface on which to apply the Captive Portal settings.

STEP 3 **Web Authentication Type:** Choose one of the following methods for web authentication. The security appliance can authenticate the users by using the local database and external AAA server (such as RADIUS, AD, and LDAP). The authentication method is derived from the user authentication settings that you specified in the Users > User Authentication page.

- **Internal:** Uses the default HotSpot Login page and requires a login.
- **Internal, no auth with accept button:** Uses the default HotSpot Login page and does not require a login. A user simply clicks the **Accept** button to access the Internet.
- **External:** Uses a custom HotSpot Login page on the specified external web server and requires a login.
- **External, no auth with accept button:** Uses a custom HotSpot Login page on the specified external web server and does not require a login. A user simply clicks the **Accept** button to access the Internet.

Note: If you chose Internal or External, you will need to use the Users > Users and Groups page to create a User Group with Captive Portal service enabled, and to add users to the group.

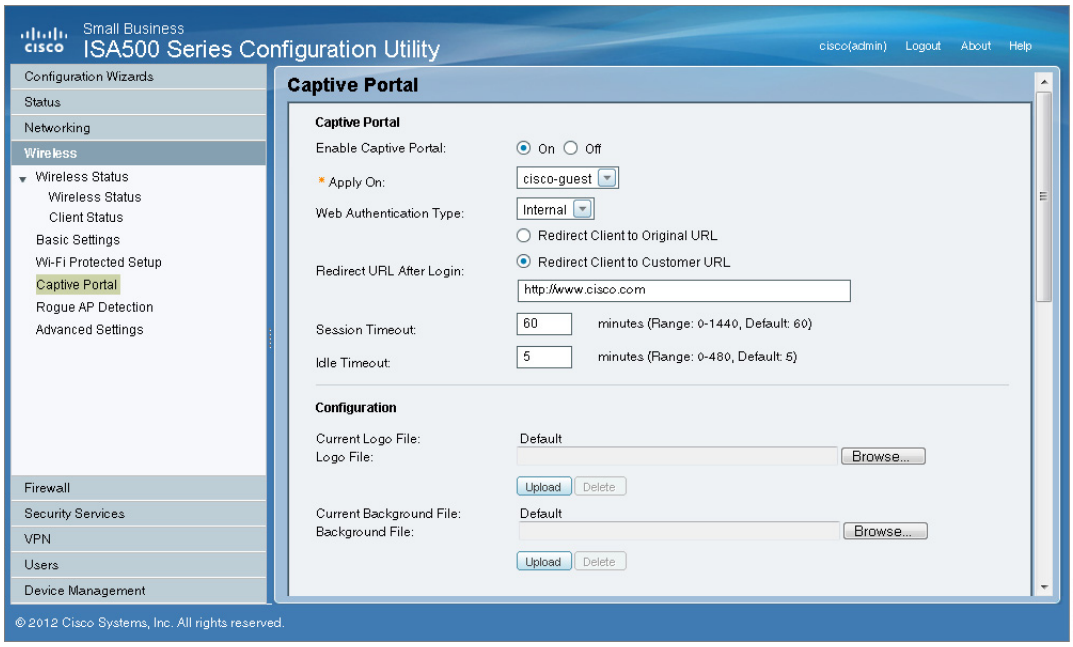
STEP 4 **Redirected URL After Login:** Choose one of the following options to determine what happens after a user leaves the portal page:

- **Redirect Client to Customer URL:** Directs the users to a particular URL (such as the URL for your company). If you choose this option, enter the desired URL in the field, including http:// or https://.
- **Redirect Client to Original URL:** Directs the users to the URL that they were trying to access originally.

STEP 5 Configure the timeout settings, or keep the default values.

- **Session Timeout:** Enter the maximum number of minutes that a wireless session can remain connected. After the timeout period elapses, the session will be terminated. Enter 0 to allow a user to remain connected without any limit. The default value is 60 minutes.

- **Idle Timeout:** Enter the maximum number of minutes that a wireless session can be idle. After the timeout period elapses, an idle session will be terminated. The default value is 5 minutes.

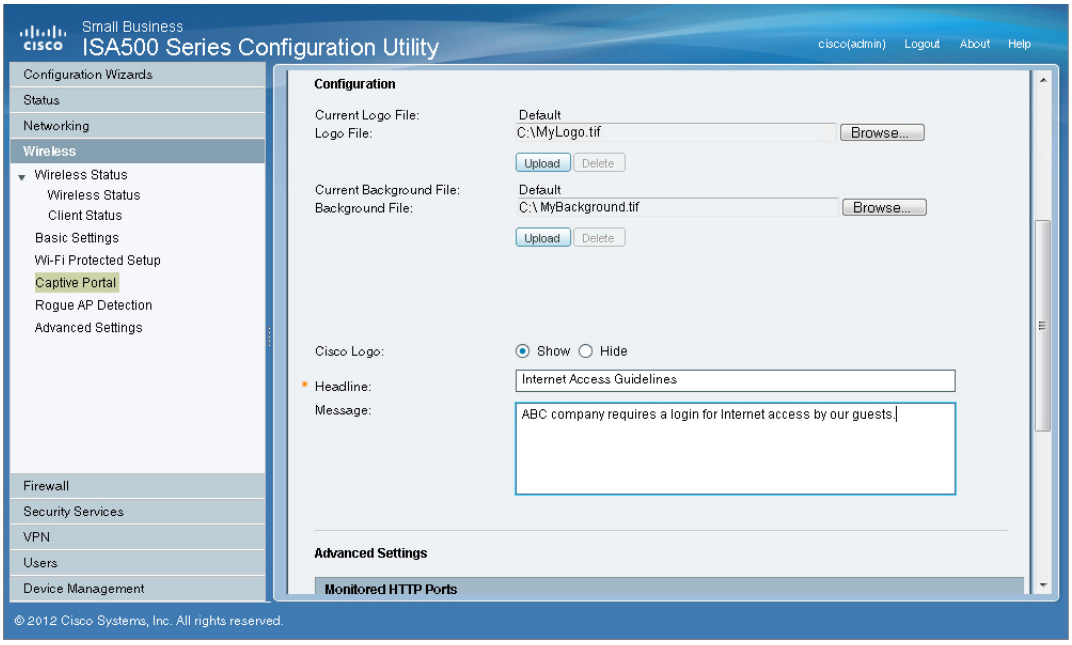


STEP 6 If you chose **Internal** or **Internal, no auth with accept button**, set up the default HotSpot Login page:

- **Logo File:** You can import an image, such as your corporate logo, to display on the login page. Click **Browse** to locate and select an image file from your local PC and then click **Upload**. To delete the loaded file, click **Delete**.
- **Background File:** You can import an image to display as the background for the login page. Click **Browse** to locate and select an image file (jpg, gif, or png) from your local PC and then click **Upload**. To delete the loaded file, click **Delete**.

  NOTE: When uploading a file, select a bmp, jpg, gif, or png file of 200KB or less. The Current Logo File field displays the filename of the file that is in use, or *Default* if no file has been uploaded for this purpose.
- **Cisco Logo:** If you want to hide the Cisco logo that appears on the login page, choose **Hide**. Otherwise, choose **Show**.
- **Headline:** If you want to create your own headline on the login page, enter the desired text in this field.

- **Message:** If you want to create your own message on the login page, enter the desired text in this field.



STEP 7 If you chose **External** or **External, no auth with accept button**, specify these settings for your external portal page:

- **Authentication Web Server:** Enter the full URL of the external web server (including https://), for example https://172.24.10.10/cgi-bin/PortalLogin.cgi.
- **Authentication Web Key:** Enter the key used to protect the username and password that the external web server sends to the security appliance for authentication.

STEP 8 If you want to use the portal for HTTP requests through other ports besides the default 80 and 443, add the ports in the **Advanced Settings > Monitored HTTP Ports** area.

NOTE: Captive Portal only monitors HTTPS requests through the port 443.

a. Click **Add**.

b. Enter the port number in the **Port** field.

c. Click **OK** to save your settings.

STEP 9 If you want to bypass the portal for certain IP addresses, add them in the **Advanced Settings > Open Domains** area.

a. Click **Add**.

b. Enter the IP address or domain name in the **Domain** field.

c. Click **OK** to save your settings.

STEP 10 Click **Save** to apply your settings.

Troubleshooting

Problem 1: User is not redirected to portal page when internal web authentication type is chosen.

Solution: Either of the following could resolve the problem:

- Check the device is connected to Captive Portals wireless network and the IP address is assigned to the device.
- Check Web Authentication Type is selected as Internal or Internal, no auth with accept button.
- Check the TCP ports on which HTTP requests are sent are added under Monitored HTTP Ports under Advanced Settings on Captive Portal page.

Problem 2: User is not redirected to portal page when internal web authentication type is chosen.

Solution: Either of the following could resolve the problem:

- Check the device is connected to Captive Portals wireless network and the IP address is assigned to the device. .
- Check Web Authentication Type is selected as External or External, no auth with accept button.
- Check the TCP ports on which HTTP requests are sent are added under Monitored HTTP Ports under Advanced Settings on Captive Portal page.
- Check the connectivity of Web-server from ISA500.
- Web-server should be able to accessed by the devices on the Captive Portal wireless network. In other words, the firewall rules associated with

the VLAN to which Captive Portal users join should be able to access the web-server.

- Check if the web-server has any issues.

Using External Web-Hosted CGI Scripts

Following is a CGI script which asks for the authentication information of a user.

The secret string programmed in the **uamsecret** variable should be configured as Authentication Web Key on the Captive portal page. Replace the **MySMB** string in the following section with your company name.

```
# !/usr/bin/perl
# chilli - ChilliSpot.org. A Wireless LAN Access Point Controller
# Copyright (C) 2003, 2004 Mondru AB.
#
# The contents of this file may be used under the terms of the GNU
# General Public License Version 2, provided that the above copyright
# notice and this permission notice is included in all copies or
# substantial portions of the software.

# Redirects from ChilliSpot daemon:
#
# Redirection when not yet or already authenticated
#   notyet:  ChilliSpot daemon redirects to login page.
#   already: ChilliSpot daemon redirects to success status page.
#
# Response to login:
#   already: Attempt to login when already logged in.
#   failed:  Login failed
#   success: Login succeded
#
# logoff:  Response to a logout


# Shared secret used to encrypt challenge with. Prevents dictionary attacks.
# You should change this to your own shared secret.
$uamsecret = "ht2eb8ej6s4et3rg1ulp";

# Uncomment the following line if you want to use ordinary user-password
# for radius authentication. Must be used together with $uamsecret.
$userpassword=1; [1]

# Our own path
$loginpath = $ENV{'SCRIPT_URL'};

use Digest::MD5  qw(md5 md5_hex md5_base64);

# Make sure that the form parameters are clean
```

```
$OK_CHARS='-a-zA-Z0-9_.@&=%!';
$| = 1;
if ($ENV{'CONTENT_LENGTH'}) {
    read (STDIN, $_, $ENV{'CONTENT_LENGTH'});
}
s/[^$OK_CHARS]/_/go;
$input = $_;


# Make sure that the get query parameters are clean
$OK_CHARS='-a-zA-Z0-9_.@&=%!';
$_ = $query=$ENV{QUERY_STRING};
s/[^$OK_CHARS]/_/go;
$query = $_;


# If she did not use https tell her that it was wrong.
if (!($ENV{HTTPS} =~ /^on$/)) {
    print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login Failed</title>[7.1]
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
</head>
<body bgColor = '#c0d8f4'>
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>[7.2]
  <center>
    Login must use encrypted connection.
  </center>
</body>
<!--
<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<WISPAccessGatewayParam
  xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
  xsi:noNamespaceSchemaLocation=
\"http://www.acmewisp.com/WISPAccessGatewayParam.xsd\">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>102</ResponseCode>
<ReplyMessage>Login must use encrypted connection</ReplyMessage>[7.3]
</AuthenticationReply>
</WISPAccessGatewayParam>
-->
</html>
";
    exit(0);
}


#Read form parameters which we care about
@array = split('&',$input);
foreach $var ( @array )
{
```

```
    @array2 = split('=',$var);
    if ($array2[0] =~ /^UserName$/) { $username = $array2[1]; }
    if ($array2[0] =~ /^Password$/) { $password = $array2[1]; }
    if ($array2[0] =~ /^challenge$/) { $challenge = $array2[1]; }
    if ($array2[0] =~ /^button$/) { $button = $array2[1]; }
    if ($array2[0] =~ /^logout$/) { $logout = $array2[1]; }
    if ($array2[0] =~ /^prelogin$/) { $prelogin = $array2[1]; }
    if ($array2[0] =~ /^res$/) { $res = $array2[1]; }
    if ($array2[0] =~ /^uamip$/) { $uamip = $array2[1]; }
    if ($array2[0] =~ /^uamport$/) { $uamport = $array2[1]; }
    if ($array2[0] =~ /^userurl$/)   { $userurl = $array2[1]; }
    if ($array2[0] =~ /^timeleft$/)  { $timeleft = $array2[1]; }
    if ($array2[0] =~ /^redirurl$/)  { $redirurl = $array2[1]; }
}

#Read query parameters which we care about
@array = split('&',$query);
foreach $var ( @array )
{
    @array2 = split('=',$var);
    if ($array2[0] =~ /^res$/)       { $res = $array2[1]; }
    if ($array2[0] =~ /^challenge$/) { $challenge = $array2[1]; }
    if ($array2[0] =~ /^uamip$/)     { $uamip = $array2[1]; }
    if ($array2[0] =~ /^uamport$/)   { $uamport = $array2[1]; }
    if ($array2[0] =~ /^reply$/)     { $reply = $array2[1]; }
    if ($array2[0] =~ /^userurl$/)   { $userurl = $array2[1]; }
    if ($array2[0] =~ /^timeleft$/)  { $timeleft = $array2[1]; }
    if ($array2[0] =~ /^redirurl$/)  { $redirurl = $array2[1]; }
}


$reply =~ s/\+/ /g;
$reply =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$userurldecode = $userurl;
$userurldecode =~ s/\+/ /g;
$userurldecode =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$redirurldecode = $redirurl;
$redirurldecode =~ s/\+/ /g;
$redirurldecode =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$password =~ s/\+/ /g;
$password =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

# If attempt to login
if ($button =~ /^Login$/) {
    $hexchal  = pack "H32", $challenge;
    if (defined $uamsecret) {
   $newchal  = md5($hexchal, $uamsecret);
    }
    else {
   $newchal  = $hexchal;
    }
    $response = md5_hex("\0", $password, $newchal);
```

```
    $pappassword = unpack "H32", ($password ^ $newchal);
#sleep 5;
print "Content-type: text/html\n\n";
print "<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">";
    if ((defined $uamsecret) && defined($userpassword)) {
   print "  <meta http-equiv=\"refresh\" content=\"0;url=
http://$uamip:$uamport/logon?username=$username&password=
$pappassword&userurl=$userurl\">";
    } else {
   print "  <meta http-equiv=\"refresh\" content=\"0;url=
http://$uamip:$uamport/logon?username=$username&response=$response&userurl=
$userurl\">";
    }
print "</head>
<body bgColor = '#c0d8f4'>";
  print "<h1 style=\"text-align: center;\">Logging in to MySMB</h1>";
  print "
  <center>
    Please wait......
  </center>
</body>
<!--
<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<WISPAccessGatewayParam
  xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
  xsi:noNamespaceSchemaLocation=
\"http://www.acmewisp.com/WISPAccessGatewayParam.xsd\">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>201</ResponseCode>
";
    if ((defined $uamsecret) && defined($userpassword)) {
   print "<LoginResultsURL>http://$uamip:$uamport/logon?username=
$username&password=$pappassword</LoginResultsURL>";
    } else {
   print "<LoginResultsURL>http://$uamip:$uamport/logon?username=
$username&response=$response&userurl=$userurl</LoginResultsURL>";
    }
print "</AuthenticationReply>
</WISPAccessGatewayParam>
-->
</html>
";
    exit(0);
}


# Default: It was not a form request
$result = 0;
```

```
# If login successful
if ($res =~ /^success$/) {
    $result = 1;
}

# If login failed
if ($res =~ /^failed$/) {
    $result = 2;
}

# If logout successful
if ($res =~ /^logoff$/) {
    $result = 3;
}

# If tried to login while already logged in
if ($res =~ /^already$/) {
    $result = 4;
}

# If not logged in yet
if ($res =~ /^notyet$/) {
    $result = 5;
}

# If login from smart client
if ($res =~ /^smartclient$/) {
    $result = 6;
}

# If requested a logging in pop up window
if ($res =~ /^popup1$/) {
    $result = 11;
}

# If requested a success pop up window
if ($res =~ /^popup2$/) {
    $result = 12;
}

# If requested a logout pop up window
if ($res =~ /^popup3$/) {
    $result = 13;
}


# Otherwise it was not a form request
# Send out an error message
if ($result == 0) {
    print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login Failed</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
```

```
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
</head>
<body bgColor = '#c0d8f4'>
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>
  <center>
    Login must be performed through MySMB daemon.
  </center>
</body>
</html>
";
    exit(0);
}

#Generate the output
print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login</title>[2.1]
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
  <SCRIPT LANGUAGE=\"JavaScript\">
    var blur = 0;
    var starttime = new Date();
    var startclock = starttime.getTime();
    var mytimeleft = 0;

    function doTime() {
      window.setTimeout( \"doTime()\", 1000 );
      t = new Date();
      time = Math.round((t.getTime() - starttime.getTime())/1000);
      if (mytimeleft) {
        time = mytimeleft - time;
        if (time <= 0) {
          window.location = \"$loginpath?res=popup3&uamip=$uamip&uamport=
$uamport\";
        }
      }
      if (time < 0) time = 0;
      hours = (time - (time % 3600)) / 3600;
      time = time - (hours * 3600);
      mins = (time - (time % 60)) / 60;
      secs = time - (mins * 60);
      if (hours < 10) hours = \"0\" + hours;
      if (mins < 10) mins = \"0\" + mins;
      if (secs < 10) secs = \"0\" + secs;
      title = \"Online time: \" + hours + \":\" + mins + \":\" + secs;
      if (mytimeleft) {
        title = \"Remaining time: \" + hours + \":\" + mins + \":\" + secs;
      }
      if(document.all || document.getElementById){
         document.title = title;
      }
      else {
        self.status = title;
```

```
      }
    }

    function popUp(URL) {
      if (self.name != \"chillispot_popup\") {
        chillispot_popup = window.open(URL, 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
500,height=375');
      }
    }

    function doOnLoad(result, URL, userurl, redirurl, timeleft) {
      if (timeleft) {
        mytimeleft = timeleft;
      }
      if ((result == 1) && (self.name == \"chillispot_popup\")) {
        doTime();
      }
      if ((result == 1) && (self.name != \"chillispot_popup\")) {
        chillispot_popup = window.open(URL, 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
500,height=375');
      }
      if ((result == 2) || result == 5) {
        document.form1.UserName.focus()
      }
      if ((result == 2) && (self.name != \"chillispot_popup\")) {
        chillispot_popup = window.open('', 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
400,height=200');
        chillispot_popup.close();
      }
      if ((result == 12) && (self.name == \"chillispot_popup\")) {
        doTime();
        if (redirurl) {
          opener.location = redirurl;
        }
        else if (userurl) {
          opener.location = userurl;
        }
        else if (opener.home) {
          opener.home();
        }
        else {
          opener.location = \"about:home\";
        }
        self.focus();
        blur = 0;
      }
      if ((result == 13) && (self.name == \"chillispot_popup\")) {
        self.focus();
        blur = 1;
      }
    }
```

```
    function doOnBlur(result) {
      if ((result == 12) && (self.name == \"chillispot_popup\")) {
        if (blur == 0) {
          blur = 1;
          self.focus();
        }
      }
    }
  </script>
</head>
<body onLoad=\"javascript:doOnLoad($result, '$loginpath?res=popup2&uamip=
$uamip&uamport=$uamport&userurl=$userurl&redirurl=$redirurl&timeleft=
$timeleft','$userurldecode', '$redirurldecode', '$timeleft')\" onBlur =
\"javascript:doOnBlur($result)\" bgColor = '#c0d8f4'>";


#      if (!window.opener) {
#        document.bgColor = '#c0d8f4';
#      }

#print "THE INPUT: $input";
#foreach $key (sort (keys %ENV)) {
#  print $key, ' = ', $ENV{$key}, "<br>\n";
#}

if ($result == 2) {
    print "
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>";[6.1]
    if ($reply) {
    print "<center> $reply </BR></BR></center>";
    }
}

if ($result == 5) {
    print "
  <h1 style=\"text-align: center;\">MySMB Login</h1>";[2.2]
}

if ($result == 2 || $result == 5) {
  print "
  <form name=\"form1\" method=\"post\" action=\"$loginpath\">
  <INPUT TYPE=\"hidden\" NAME=\"challenge\" VALUE=\"$challenge\">
  <INPUT TYPE=\"hidden\" NAME=\"uamip\" VALUE=\"$uamip\">
  <INPUT TYPE=\"hidden\" NAME=\"uamport\" VALUE=\"$uamport\">
  <INPUT TYPE=\"hidden\" NAME=\"userurl\" VALUE=\"$userurldecode\">
  <center>
  <table border=\"0\" cellpadding=\"5\" cellspacing=\"0\" style=\"width:
217px;\">
    <tbody>
      <tr>
        <td align=\"right\">Username:</td>[2.3]
        <td><input STYLE=\"font-family: Arial\" type=\"text\" name=
\"UserName\" size=\"20\" maxlength=\"128\"></td>
      </tr>
      <tr>
```

```
        <td align=\"right\">Password:</td>[2.4]
        <td><input STYLE=\"font-family: Arial\" type=\"password\" name=
\"Password\" size=\"20\" maxlength=\"128\"></td>
      </tr>
      <tr>
        <td align=\"center\" colspan=\"2\" height=\"23\"><input type=
\"submit\" name=\"button\" value=\"Login\"[2.5] onClick=
\"javascript:popUp('$loginpath?res=popup1&uamip=$uamip&uamport=
$uamport')\"></td>
      </tr>
    </tbody>
  </table>
  </center>
  </form>
</body>
</html>";
}

if ($result == 1) {
  print "
  <h1 style=\"text-align: center;\">Logged in to MySMB</h1>";[8.1]

  if ($reply) {
      print "<center> $reply </BR></BR></center>";
  }

  print "
  <center>
    <a href=\"http://$uamip:$uamport/logoff\">Logout</a>[8.2]
  </center>
</body>
</html>";
}

if (($result == 4) || ($result == 12)) {
  print "
  <h1 style=\"text-align: center;\">Logged in to MySMB</h1>[4.1]
  <center>
    <a href=\"http://$uamip:$uamport/logoff\">Logout</a>[4.2]
  </center>
</body>
</html>";
}


if ($result == 11) {
  print "<h1 style=\"text-align: center;\">Logging in to MySMB</h1>[3.1]";
  print "
  <center>
    Please wait..... [3.2]
  </center>
</body>
</html>";
}
```

```
if (($result == 3) || ($result == 13)) {
    print "
  <h1 style=\"text-align: center;\">Logged out from MySMB</h1>[5.1]
  <center>
    <a href=\"http://$uamip:$uamport/prelogin\">Login</a>[5.2]
  </center>
</body>
</html>";
}


exit(0);
```

CGI Source Code Example: No Authentication and Accept Button

Following is a CGI script which presents a Accept button on the portal page.

The secret string programmed in **`uamsecret`** variable should be configured as Authentication Web Key on the Captive portal page. Replace the **MySMB** string in the following section with your company name.

```
#!/usr/bin/perl

# chilli - ChilliSpot.org. A Wireless LAN Access Point Controller
# Copyright (C) 2003, 2004 Mondru AB.
#
# The contents of this file may be used under the terms of the GNU
# General Public License Version 2, provided that the above copyright
# notice and this permission notice is included in all copies or
# substantial portions of the software.

# Redirects from ChilliSpot daemon:
#
# Redirection when not yet or already authenticated
#   notyet:  ChilliSpot daemon redirects to login page.
#   already: ChilliSpot daemon redirects to success status page.
#
# Response to login:
#   already: Attempt to login when already logged in.
#   failed:  Login failed
#   success: Login succeded
#
# logoff:  Response to a logout


# Shared secret used to encrypt challenge with. Prevents dictionary attacks.
# You should change this to your own shared secret.
#$uamsecret = "ht2eb8ej6s4et3rg1ulp";
```

```
$uamsecret = "gemteksmb";

# Uncomment the following line if you want to use ordinary user-password
# for radius authentication. Must be used together with $uamsecret.
$userpassword=1;

# Our own path
$loginpath = $ENV{'SCRIPT_URL'};

use Digest::MD5  qw(md5 md5_hex md5_base64);

# Make sure that the form parameters are clean
$OK_CHARS='-a-zA-Z0-9_.@&=%!';
$| = 1;
if ($ENV{'CONTENT_LENGTH'}) {
    read (STDIN, $_, $ENV{'CONTENT_LENGTH'});
}
s/[^$OK_CHARS]/_/go;
$input = $_;


# Make sure that the get query parameters are clean
$OK_CHARS='-a-zA-Z0-9_.@&=%!';
$_ = $query=$ENV{QUERY_STRING};
s/[^$OK_CHARS]/_/go;
$query = $_;


# If she did not use https tell her that it was wrong.
if (!($ENV{HTTPS} =~ /^on$/)) {
    print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login Failed</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
</head>
<body bgColor = '#c0d8f4'>
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>
  <center>
    Login must use encrypted connection.
  </center>
</body>
<!--
<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<WISPAccessGatewayParam
  xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
  xsi:noNamespaceSchemaLocation=
\"http://www.acmewisp.com/WISPAccessGatewayParam.xsd\">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>102</ResponseCode>
<ReplyMessage>Login must use encrypted connection</ReplyMessage>
</AuthenticationReply>
```

```
</WISPAccessGatewayParam>
-->
</html>
";
    exit(0);
}


#Read form parameters which we care about
@array = split('&',$input);
foreach $var ( @array )
{
    @array2 = split('=',$var);
    if ($array2[0] =~ /^UserName$/) { $username = $array2[1]; }
    if ($array2[0] =~ /^Password$/) { $password = $array2[1]; }
    if ($array2[0] =~ /^challenge$/) { $challenge = $array2[1]; }
    if ($array2[0] =~ /^button$/) { $button = $array2[1]; }
    if ($array2[0] =~ /^logout$/) { $logout = $array2[1]; }
    if ($array2[0] =~ /^prelogin$/) { $prelogin = $array2[1]; }
    if ($array2[0] =~ /^res$/) { $res = $array2[1]; }
    if ($array2[0] =~ /^uamip$/) { $uamip = $array2[1]; }
    if ($array2[0] =~ /^uamport$/) { $uamport = $array2[1]; }
    if ($array2[0] =~ /^userurl$/)   { $userurl = $array2[1]; }
    if ($array2[0] =~ /^timeleft$/)  { $timeleft = $array2[1]; }
    if ($array2[0] =~ /^redirurl$/)  { $redirurl = $array2[1]; }
}

#Read query parameters which we care about
@array = split('&',$query);
foreach $var ( @array )
{
    @array2 = split('=',$var);
    if ($array2[0] =~ /^res$/)       { $res = $array2[1]; }
    if ($array2[0] =~ /^challenge$/) { $challenge = $array2[1]; }
    if ($array2[0] =~ /^uamip$/)     { $uamip = $array2[1]; }
    if ($array2[0] =~ /^uamport$/)   { $uamport = $array2[1]; }
    if ($array2[0] =~ /^reply$/)     { $reply = $array2[1]; }
    if ($array2[0] =~ /^userurl$/)   { $userurl = $array2[1]; }
    if ($array2[0] =~ /^timeleft$/)  { $timeleft = $array2[1]; }
    if ($array2[0] =~ /^redirurl$/)  { $redirurl = $array2[1]; }
}


$reply =~ s/\+/ /g;
$reply =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$userurldecode = $userurl;
$userurldecode =~ s/\+/ /g;
$userurldecode =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$redirurldecode = $redirurl;
$redirurldecode =~ s/\+/ /g;
$redirurldecode =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

$password =~ s/\+/ /g;
```

```
$password =~s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/seg;

# If attempt to login
if ($button =~ /^Accept$/) {
    $hexchal  = pack "H32", $challenge;
    if (defined $uamsecret) {
   $newchal  = md5($hexchal, $uamsecret);
    }
    else {
   $newchal  = $hexchal;
    }
    $response = md5_hex("\0", $password, $newchal);
    $pappassword = unpack "H32", ($password ^ $newchal);
#sleep 5;
print "Content-type: text/html\n\n";
print "<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">";
    if ((defined $uamsecret) && defined($userpassword)) {
   print "  <meta http-equiv=\"refresh\" content=\"0;url=
http://$uamip:$uamport/logon?username=$username&password=
$pappassword&userurl=$userurl\">";
    } else {
   print "  <meta http-equiv=\"refresh\" content=\"0;url=
http://$uamip:$uamport/logon?username=$username&response=$response&userurl=
$userurl\">";
    }
print "</head>
<body bgColor = '#c0d8f4'>";
  print "<h1 style=\"text-align: center;\">Logging in to MySMB</h1>";
  print "
  <center>
    Please wait......
  </center>
</body>
<!--
<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<WISPAccessGatewayParam
  xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\"
  xsi:noNamespaceSchemaLocation=
\"http://www.acmewisp.com/WISPAccessGatewayParam.xsd\">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>201</ResponseCode>
";
    if ((defined $uamsecret) && defined($userpassword)) {
   print "<LoginResultsURL>http://$uamip:$uamport/logon?username=
$username&password=$pappassword</LoginResultsURL>";
    } else {
   print "<LoginResultsURL>http://$uamip:$uamport/logon?username=
$username&response=$response&userurl=$userurl</LoginResultsURL>";
    }
```

```
print "</AuthenticationReply>
</WISPAccessGatewayParam>
-->
</html>
";
    exit(0);
}


# Default: It was not a form request
$result = 0;

# If login successful
if ($res =~ /^success$/) {
    $result = 1;
}

# If login failed
if ($res =~ /^failed$/) {
    $result = 2;
}

# If logout successful
if ($res =~ /^logoff$/) {
    $result = 3;
}

# If tried to login while already logged in
if ($res =~ /^already$/) {
    $result = 4;
}

# If not logged in yet
if ($res =~ /^notyet$/) {
    $result = 5;
}

# If login from smart client
if ($res =~ /^smartclient$/) {
    $result = 6;
}

# If requested a logging in pop up window
if ($res =~ /^popup1$/) {
    $result = 11;
}

# If requested a success pop up window
if ($res =~ /^popup2$/) {
    $result = 12;
}

# If requested a logout pop up window
if ($res =~ /^popup3$/) {
    $result = 13;
```

```
}


# Otherwise it was not a form request
# Send out an error message
if ($result == 0) {
    print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login Failed</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
</head>
<body bgColor = '#c0d8f4'>
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>
  <center>
    Login must be performed through MySMB daemon.
  </center>
</body>
</html>
";
    exit(0);
}

#Generate the output
print "Content-type: text/html\n\n
<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.01 Transitional//EN\">
<html>
<head>
  <title>MySMB Login</title>
  <meta http-equiv=\"Cache-control\" content=\"no-cache\">
  <meta http-equiv=\"Pragma\" content=\"no-cache\">
  <SCRIPT LANGUAGE=\"JavaScript\">
    var blur = 0;
    var starttime = new Date();
    var startclock = starttime.getTime();
    var mytimeleft = 0;

    function doTime() {
      window.setTimeout( \"doTime()\", 1000 );
      t = new Date();
      time = Math.round((t.getTime() - starttime.getTime())/1000);
      if (mytimeleft) {
        time = mytimeleft - time;
        if (time <= 0) {
          window.location = \"$loginpath?res=popup3&uamip=$uamip&uamport=
$uamport\";
        }
      }
      if (time < 0) time = 0;
      hours = (time - (time % 3600)) / 3600;
      time = time - (hours * 3600);
      mins = (time - (time % 60)) / 60;
      secs = time - (mins * 60);
```

```
      if (hours < 10) hours = \"0\" + hours;
      if (mins < 10) mins = \"0\" + mins;
      if (secs < 10) secs = \"0\" + secs;
      title = \"Online time: \" + hours + \":\" + mins + \":\" + secs;
      if (mytimeleft) {
        title = \"Remaining time: \" + hours + \":\" + mins + \":\" + secs;
      }
      if(document.all || document.getElementById){
         document.title = title;
      }
      else {
        self.status = title;
      }
    }

    function popUp(URL) {
      if (self.name != \"chillispot_popup\") {
        chillispot_popup = window.open(URL, 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
500,height=375');
      }
    }

    function doOnLoad(result, URL, userurl, redirurl, timeleft) {
   if (timeleft) {
       mytimeleft = timeleft;
      }
      if ((result == 1) && (self.name == \"chillispot_popup\")) {
        doTime();
      }
      if ((result == 1) && (self.name != \"chillispot_popup\")) {
        chillispot_popup = window.open(URL, 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
500,height=375');
      }
      if ((result == 2) || result == 5) {
        //document.form1.UserName.focus()
      }
      if ((result == 2) && (self.name != \"chillispot_popup\")) {
        chillispot_popup = window.open('', 'chillispot_popup', 'toolbar=
0,scrollbars=0,location=0,statusbar=0,menubar=0,resizable=0,width=
400,height=200');
        chillispot_popup.close();
      }
      if ((result == 12) && (self.name == \"chillispot_popup\")) {
        doTime();
        if (redirurl) {
          opener.location = redirurl;
        }
        else if (userurl) {
          opener.location = userurl;
        }
        else if (opener.home) {
          opener.home();
        }
```

```
        else {
          opener.location = \"about:home\";
        }
        self.focus();
        blur = 0;
      }
      if ((result == 13) && (self.name == \"chillispot_popup\")) {
        self.focus();
        blur = 1;
      }
    }

    function doOnBlur(result) {
      if ((result == 12) && (self.name == \"chillispot_popup\")) {
        if (blur == 0) {
          blur = 1;
          self.focus();
        }
      }
    }
  </script>
</head>
<body onLoad=\"javascript:doOnLoad($result, '$loginpath?res=popup2&uamip=
$uamip&uamport=$uamport&userurl=$userurl&redirurl=$redirurl&timeleft=
$timeleft','$userurldecode', '$redirurldecode', '$timeleft')\" onBlur =
\"javascript:doOnBlur($result)\" bgColor = '#c0d8f4'>";


#      if (!window.opener) {
#        document.bgColor = '#c0d8f4';
#      }

#print "THE INPUT: $input";
#foreach $key (sort (keys %ENV)) {
#  print $key, ' = ', $ENV{$key}, "<br>\n";
#}

if ($result == 2) {
    print "
  <h1 style=\"text-align: center;\">MySMB Login Failed</h1>";
    if ($reply) {
    print "<center> $reply </BR></BR></center>";
    }
}

if ($result == 5) {
    print "
  <h1 style=\"text-align: center;\">MySMB Login</h1>";
}

if ($result == 2 || $result == 5) {
  print "
  <form name=\"form1\" method=\"post\" action=\"$loginpath\">
  <INPUT TYPE=\"hidden\" NAME=\"challenge\" VALUE=\"$challenge\">
  <INPUT TYPE=\"hidden\" NAME=\"uamip\" VALUE=\"$uamip\">
```

```
  <INPUT TYPE=\"hidden\" NAME=\"uamport\" VALUE=\"$uamport\">
  <INPUT TYPE=\"hidden\" NAME=\"userurl\" VALUE=\"$userurldecode\">
  <INPUT TYPE=\"hidden\" NAME=\"UserName\" VALUE=\"\">
  <INPUT TYPE=\"hidden\" NAME=\"Password\" VALUE=\"\">
  <center>
  <table border=\"0\" cellpadding=\"5\" cellspacing=\"0\" style=\"width:
217px;\">
    <tbody>
      <tr>
        <td align=\"center\" colspan=\"2\" height=\"23\"><input type=
\"submit\" name=\"button\" value=\"Accept\" onClick=
\"javascript:popUp('$loginpath?res=popup1&uamip=$uamip&uamport=
$uamport')\"></td>
      </tr>
    </tbody>
  </table>
  </center>
  </form>
</body>
</html>";
}

if ($result == 1) {
  print "
  <h1 style=\"text-align: center;\">Logged in to MySMB</h1>";

  if ($reply) {
      print "<center> $reply </BR></BR></center>";
  }

  print "
  <center>
    <a href=\"http://$uamip:$uamport/logoff\">Logout</a>
  </center>
</body>
</html>";
}

if (($result == 4) || ($result == 12)) {
  print "
  <h1 style=\"text-align: center;\">Logged in to MySMB</h1>
  <center>
    <a href=\"http://$uamip:$uamport/logoff\">Logout</a>
  </center>
</body>
</html>";
}


if ($result == 11) {
  print "<h1 style=\"text-align: center;\">Logging in to MySMB</h1>";
  print "
  <center>
    Please wait......
  </center>
```

```
</body>
</html>";
}


if (($result == 3) || ($result == 13)) {
    print "
  <h1 style=\"text-align: center;\">Logged out from MySMB</h1>
  <center>
    <a href=\"http://$uamip:$uamport/prelogin\">Login</a>
  </center>
</body>
</html>";
}


exit(0);
```

Related Information

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Cisco Small Business Firmware Downloads	www.cisco.com/go/isa500software
Cisco Small Business Open Source Requests	www.cisco.com/go/smallbiz_opensource_request
Documentation	
Product Documentation	www.cisco.com/go/isa500resources
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb

Cisco Small Business Home	www.cisco.com/smb

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.

78-21182-01

Configuring Wireless Rogue AP Detection

A Rogue AP is an access point connected to your network without authorization. It is not under the management of your network administrators and does not necessarily conform to your network security policies.

The security appliance provides proactive Rogue AP Detection in the 2.4-GHz band. Rogue AP Detection is able to discover, detect, and report unauthorized access points. You can specify an authorized access point by its MAC address.

STEP 1 Click **Wireless > Rogue AP Detection**.

The Rogue AP Detection window opens.

STEP 2 Click **On** to enable Rogue AP Detection, or click **Off** to disable it.

STEP 3 If you enable Rogue AP Detection, all rogue access points detected by the security appliance in the vicinity of the network appear in the list of Detected Rogue Access Points. The MAC address of the detected access point is displayed. You can locate the rogue access points by their MAC addresses and monitor them until they are eliminated or authorized. Click **Refresh** to update the data.

STEP 4 If an access point listed as a rogue is actually a legitimate access point, you can click **Grant Access** to set it as an authorized access point. The granted access point is moved to the list of Authorized Access Points.

STEP 5 The security appliance will not detect the authorized access points.

- To add an authorized access point, click **Add**. Enter the MAC address of the access point and click **OK**. You can specify up to 128 authorized access points.
- To delete an authorized access point from the list, click the **Delete** (x) icon.

- To change the MAC address of an authorized access point, click the **Edit** (pencil) icon.
- To export the list of authorized access points to a file, click **Export**.
- To import the list of authorized access points from a file, click **Import**.

  Choose whether to replace the existing list of Authorized Access Points or add the entries in the imported file to the list of Authorized Access Points.

  - Click **Replace** to import the list and replace the entire contents of the list of Authorized Access Points. Click **Browse** to locate the file and click **OK**.
  - Click **Merge** to import the list and add the access points in the imported file to the access points currently displayed in the list of Authorized Access Points. Click **Browse** to locate the file and click **OK**.

  After the import is complete, the screen refreshes and the MAC addresses of the imported access points appear in the list of Authorized Access Points.

STEP 6 Click **Save** to apply your settings.

Advanced Radio Settings

Use the Advanced Settings page to specify the advanced radio settings.

NOTE This page is available if the wireless radio is enabled on the Basic Settings page.

STEP 1 Click **Wireless > Advanced Settings**.

STEP 2 Enter the following information:

- **Guard Interval:** Choose either Long (800 ns) or Short (400 ns) that the security appliance will retry a frame transmission that fails.

  NOTE: The short frame is only available when the specified wireless mode includes 802.11n.

- **CTS Protection Mode:** CTS (Clear-To-Send) Protection Mode function boosts the ability of the SSID to catch all Wireless-G transmissions but will severely decrease performance.

- Select the **AUTO** radio button if you want the security appliance to perform a CTS handshake before transmitting a packet. This mode can minimize collisions among hidden stations.
- Select the **Disabled** radio button if you want to permanently disable this feature.

- **Power Output:** You can adjust the output power of the access point to get the appropriate coverage for your wireless network. Choose the level that you need for your environment. If you are not sure of which setting to select, then use the default setting, 100%.
- **Beacon Interval:** Beacon frames are transmitted by the access point at regular intervals to announce the existence of the wireless network. Set the interval by entering a value in milliseconds. Enter a value from 20 to 999 ms. The default value is 100 ms, which means that beacon frames are sent every 100 ms.
- **DTIM Interval:** The Delivery Traffic Information Map (DTIM) message is an element that is included in some beacon frames. It indicates that the client stations are currently sleeping in low-power mode and have buffered data on the access point awaiting pickup. Set the interval by entering a value in beacon frames. Enter a value from 1 to 255. The default value is 1, which means that the DTIM message is included in every second beacon frame.
- **RTS Threshold:** The RTS threshold determines the packet size that requires a Request To Send (RTS)/Clear To Send (CTS) handshake before sending. A low threshold setting can be useful in areas where many client devices are associating with the wireless device, or in areas where the clients are far apart and can detect only the access point but not other clients. Although a low threshold value consumes more bandwidth and reduces the throughput of the packet, frequent RTS packets can help the network recover from interference or collisions. Set the threshold by entering the packet size in bytes. Enter a value from 1 to 2347. The default value is 2347, which effectively disables RTS.
- **Fragmentation Threshold:** The fragmentation threshold is the frame length that requires packets to be broken up (fragmented) into two or more frames. Setting a lower value can reduce collisions because collisions occur more often in the transmission of long frames, which occupy the channel for a longer time. Use a low setting in areas where communication is poor or where there is a great deal of radio interference. Set the threshold by entering the frame length in bytes. Enter a value from 256 to 2346. The default value is 2346, which effectively disables fragmentation.

STEP 3 Click **Save** to apply your settings.

6

Firewall

This chapter describes how to configure firewall rules that control inbound and outbound traffic and to specify other settings that protect your network. It includes the following sections:

- **Configuring Firewall Rules to Control Inbound and Outbound Traffic, page 252**
- **Configuring NAT Rules to Securely Access a Remote Network, page 261**
- **Firewall and NAT Rule Configuration Examples, page 274**
- **Configuring Content Filtering to Control Internet Access, page 281**
- **Configuring MAC Address Filtering to Permit or Block Traffic, page 285**
- **Configuring IP-MAC Binding to Prevent Spoofing, page 286**
- **Configuring Attack Protection, page 287**
- **Configuring Session Limits, page 288**
- **Configuring Application Level Gateway, page 289**

To access the Firewall pages, click **Firewall** in the left hand navigation pane.

Configuring Firewall Rules to Control Inbound and Outbound Traffic

The zone-based firewall can permit or deny inbound or outbound traffic based on the zone, service, source and destination address, and schedule.

Refer to the following topics:

- **Default Firewall Settings, page 254**
- **Priorities of Firewall Rules, page 255**
- **Preliminary Tasks for Configuring Firewall Rules, page 255**
- **General Firewall Settings, page 256**
- **Configuring a Firewall Rule, page 257**
- **Configuring a Firewall Rule to Allow Multicast Traffic, page 259**
- **Configuring Firewall Logging Settings, page 260**

About Security Zones

A security zone is a group of interfaces to which a security policy can be applied to control traffic between zones. For ease of deployment, the Cisco ISA500 has several predefined zones with default security settings to protect your network. You can create additional zones as needed.

Each zone has an associated security level. The security level represents the level of trust, from low (0) to high (100). Default firewall rules are created for all predefined zones and your new zones, based on these security levels. For example, by default all traffic from the LAN zone (with a Trusted security level) to the WAN zone (with an Untrusted security level) is allowed but traffic from the WAN (Untrusted) zone to the LAN (Trusted) zone is blocked. You can create and modify firewall rules to specify the permit or block action for specified services, source and destination addresses, and schedules.

To learn more, see the **Security Levels and Predefined Zones** table.

Security Levels and Predefined Zones

Security Level	Description	Predefined Zones
Trusted (100)	Highest level of trust. By default, the DEFAULT VLAN is mapped to the predefined LAN zone. You can group one or more VLANs into a Trusted zone.	LAN
VPN (75)	Higher level of trust than a public zone, but a lower level of trust than a trusted zone. This security level is used exclusively for VPN connections. All traffic is encrypted.	VPN SSLVPN
Public (50)	Higher level of trust than a guest zone, but a lower level of trust than a VPN zone.	DMZ
Guest (25)	Higher level of trust than an untrusted zone, but a lower level of trust than a public zone.	GUEST
Untrusted (0)	Lowest level of trust. By default, the WAN1 interface is mapped to the WAN zone. If you are using the secondary WAN (WAN2), you can map it to the WAN zone or any other untrusted zone.	WAN
Voice	Designed exclusively for voice traffic. Incoming and outgoing traffic is optimized for voice operations. For example, assign Cisco IP Phones to the VOICE zone.	VOICE

Default Firewall Settings

By default, the firewall prevents all traffic from a lower security zone to a higher security zone (commonly known as Inbound) and allows all traffic from a higher security zone to a lower security zone (commonly known as Outbound).

For example, all traffic from the LAN (trusted zone) to the WAN (untrusted zone) is permitted, and traffic from the WAN (untrusted zone) to the DMZ (public zone) is blocked.

When you create a new zone, such as a Data zone, firewall rules are automatically generated to permit or block traffic between that zone and other zones, based on the security levels for the **From** and **To** zones.

The following table displays the default access control settings for traffic between the zones in the same or different security levels.

From/To	Trusted(100)	VPN(75)	Public(50)	Guest(25)	Untrusted(0)
Trusted(100)	Deny	Permit	Permit	Permit	Permit
VPN(75)	Deny	Deny	Permit	Permit	Permit
Public(50)	Deny	Deny	Deny	Permit	Permit
Guest(25)	Deny	Deny	Deny	Deny	Permit
Untrusted(0)	Deny	Deny	Deny	Deny	Deny

If you want to alter the default behaviors—for example, allowing some inbound access to your network (WAN to LAN) or blocking some outbound traffic from your network (LAN to WAN)—you must create firewall rules.

Use the Default Policies page to view the default firewall behaviors for all predefined zones and new zones.

STEP 1 Click **Firewall > Access Control > Default Policies**.

STEP 2 Click the triangle to expand or contract the default access control settings for a specific zone. The following behaviors are defined for all predefined zones.

From/To	LAN	VOICE	VPN	SSLVPN	DMZ	GUEST	WAN
LAN	N/A	Deny	Permit	Permit	Permit	Permit	Permit

VOICE	Deny	N/A	Permit	Permit	Permit	Permit	Permit
VPN	Deny	Deny	N/A	Deny	Permit	Permit	Permit
SSLVPN	Deny	Deny	Deny	N/A	Permit	Permit	Permit
DMZ	Deny	Deny	Deny	Deny	N/A	Permit	Permit
GUEST	Deny	Deny	Deny	Deny	Deny	N/A	Permit
WAN	Deny	Deny	Deny	Deny	Deny	Deny	N/A

NOTE ACL rules are applicable for inter-VLAN traffic, whether within a zone or between zones. You cannot set ACL rules for intra-VLAN traffic, such as LAN to LAN.

Priorities of Firewall Rules

The security appliance includes three types of firewall rules:

- **Default firewall rules:** The firewall rules that are defined on the security appliance for all predefined zones and new zones. The default firewall rules cannot be deleted nor edited.
- **Custom firewall rules:** The firewall rules that are configured by the users. The security appliance supports up to 100 custom firewall rules.
- **VPN firewall rules:** The firewall rules that are automatically generated by the zone access control settings in your VPN configurations. The VPN firewall rules cannot be edited in the Firewall > Access Control > ACL Rules page. To edit the zone access control settings in your VPN configurations, go to the VPN pages.

All firewall rules are sorted by the priority. The custom firewall rules have the highest priority. The VPN firewall rules have higher priorities than the default firewall rules, but lower than the custom firewall rules.

Preliminary Tasks for Configuring Firewall Rules

Depending on the firewall settings that you want to use, you may need to complete the following tasks before you configure firewall rules:

- To create a firewall rule that applies only to a specific zone except the predefined zones, first create the zone. See Configuring Zones, page 146.

- To create a firewall rule that applies to a specific service or service group, first create the service or service group. See Service Management, page 177.
- To create a firewall rule that applies only to a specific address or address group, first create the address or address group. See Address Management, page 175.
- To create a firewall rule that applies only at a specific day and time, first create the schedule. See Configuring Schedules, page 449.

General Firewall Settings

STEP 1 Click **Firewall > Access Control > ACL Rules**.

The ACL Rules window opens. The firewall rules appear in the ACL Control List (ACL) table. The table includes all firewall rules for controlling traffic from a particular zone to a particular destination.

STEP 2 The firewall rules are sorted by the priority. You can reorder the custom firewall rules by the priority. You can move a rule up, move a rule down, or move it to a specified location in the list.

- To move the rule up one position, click the **Move up** icon.
- To move the rule down one position, click the **Move down** icon.
- To move the rule to a specific location, click the **Move** icon and enter the target index number to move the selected rule to.

  For example: A target index of 2 moves the rule to position 2 and moves the other rules down to position 3 in the list.

  NOTE: You cannot reorder the default firewall rules and VPN firewall rules. The custom firewall rules cannot be moved lower than the default firewall rules and VPN firewall rules.

STEP 3 To view the list of firewall rules that belong to the same group, choose the source and destination from the **From Zone** and **To Zone** drop-down lists and click **Apply**. Only the rules for the specified zones appear.

For example: If you choose WAN from the **From Zone** drop-down list and choose LAN from the **To Zone** drop-down list, only the firewall rules from WAN to LAN appear.

STEP 4 You can perform other tasks for firewall rules:

- Check **Enable** to enable a firewall rule, or uncheck this box to disable it. By default, all default firewall rules are enabled.
- To add a new entry, click the **Add** button.
- To edit an entry, click the **Edit** (pencil) icon.
- To delete an entry, click the **Delete** (x) icon.
- To delete multiple entries, check them and click the **Delete** button.
- Check **Log** to log the event when a firewall rule is hit. For information on configuring firewall logging settings, see **Configuring Firewall Logging Settings, page 260**.
- To permit traffic access, choose **Permit**. To deny traffic access, choose **Deny**. To increase the Hit Count number by one when the packet hits the firewall rule, choose **Accounting**.
- To view the type of a firewall rule, point your mouse cursor to the **Detail** icon.
- To set the values in the Hit Count column for all firewall rules to zero, click **Reset**.
- To manually refresh the data in the table, click **Refresh**.

NOTE: The default firewall rules cannot be disabled, deleted, edited, nor moved.

Configuring a Firewall Rule

This section describes how to configure a firewall rule to control inbound or outbound traffic.

NOTE For detailed firewall configuration examples, see **Firewall and NAT Rule Configuration Examples, page 274**.

STEP 1 Click **Firewall > Access Control > ACL Rules**.

The ACL Rules window opens.

STEP 2 To add a new firewall rule, click **Add**.

The Rule - Add/Edit window opens.

STEP 3 Enter the following information:

- **Enable:** Click **On** to enable the firewall rule, or click **Off** to create only the firewall rule.
- **From Zone:** Choose the source zone for traffic that is covered by this firewall rule. For example, choose **DMZ** if traffic is coming from a server on your DMZ.
- **To Zone:** Choose the destination zone for traffic that is covered by this firewall rule. For example, choose **WAN** if traffic is going to the Internet.

  NOTE: Only the existing zones are selectable. To create new zones, go to the **Networking > Zone** page. For information on configuring zones, see Configuring Zones, page 146.
- **Services:** Choose an existing service or service group that is covered by this firewall rule. If the service or service group that you want is not in the list, choose **Create a new service** to create a new service object or choose **Create a new service group** to create a new service group object. To maintain the service and service group objects, go to the **Networking > Service Management** page. See Service Management, page 177.
- **Source Address:** Choose an existing address or address group as the source address or network that is covered by this firewall rule.
- **Destination Address**: Choose an existing address or address group as the destination address or network that is covered by this firewall rule.

  If the address or address group that you want is not in the list, choose **Create a new address** to create a new address object, or choose **Create a new address group** to create a new address group object. To maintain the address and address group objects, go to the **Networking > Address Management** page. See Address Management, page 175.
- **Schedule:** By default, the firewall rule is always on. If you want to keep the firewall rule active at a specific day and time, choose the schedule for the firewall rule. If the schedule that you want is not in the list, choose **Create a new schedule** to create a new schedule. To maintain the schedules, go to the **Device Management > Schedules** page. See Configuring Schedules, page 449.
- **Log:** Click **On** to log the event when a firewall rule is hit. For information on configuring firewall logging settings, see Configuring Firewall Logging Settings, page 260.

- **Match Action:** Choose the action for traffic when the packet hits the firewall rule.
  - **Deny:** Deny access.
  - **Permit:** Permit access.
  - **Accounting:** Increase the Hit Count number by one when the packet hits the firewall rule.

STEP 4 Click **OK** to save your settings.

STEP 5 Click **Save** to apply your settings.

NOTE In addition to firewall rules, you can use the following methods to control traffic:

- Prevent common types of attacks. See **Configuring Attack Protection, page 287**.
- Allow or block traffic from specified MAC addresses. See **Configuring MAC Address Filtering to Permit or Block Traffic, page 285**
- Associate the IP address with the MAC address to prevent spoofing. See **Configuring IP-MAC Binding to Prevent Spoofing, page 286**
- Allow or block the websites that contain specific domains or URL keywords. See **Configuring Content Filtering to Control Internet Access, page 281**.

Configuring a Firewall Rule to Allow Multicast Traffic

By default, multicast traffic from Any zone to Any zone is blocked by the firewall. To enable multicast traffic, you must first uncheck **Block Multicast Packets** in the **Firewall > Attack Protection** page, and then manually create firewall rules to allow multicast forwarding from a specific zone to other zones. The security appliance predefines a multicast address (**IPv4_Multicast**) for this purpose.

For example, IGMP Proxy can be active from WAN zone to LAN zone. When you enable IGMP Proxy and want to receive multicast packets from WAN zone to LAN zone, you must uncheck **Block Multicast Packets** in the **Firewall > Attack Protection** page, and then create a firewall rule to permit multicast traffic from WAN zone to LAN zone.

This section provides a configuration example about how to create a WAN-to-LAN firewall rule to permit multicast traffic by using the predefined multicast address object.

STEP 1 Click **Firewall > Access Control > ACL Rules**.

STEP 2 Click **Add** to add a new firewall rule.

The Rule - Add/Edit window opens.

STEP 3 Enter the following information:

- **Enable:** Click **On** to enable the firewall rule.
- **From Zone:** Choose **WAN** as the source zone of traffic.
- **To Zone:** Choose **LAN** as the destination zone of traffic.
- **Services:** Choose **ANY** for this firewall rule.
- **Source Address:** Choose **ANY** as the source address.
- **Destination Address:** Choose the predefined multicast address called "**IPv4_Multicast**" as the destination address.
- **Schedule:** Choose **Always On** for this firewall rule.
- **Log:** Click **Off** for this firewall rule. We recommend that you disable the Log feature for a multicast firewall rule.
- **Match Action:** Choose **Permit** to allow access.

STEP 4 Click **OK** to save your settings.

STEP 5 Click **Save** to apply your settings.

Configuring Firewall Logging Settings

Perform the following steps to log the firewall events and view firewall logs:

STEP 1 Enable the Log feature for firewall rules. See **Configuring a Firewall Rule, page 257**.

STEP 2 Go to the **Device Management > Logs > Log Settings** page to configure the log settings. You must enable the Log feature, set the log buffer size, and specify the

Email Alert, Remote Logs, and Local Log settings if you want to send firewall logs to a specified email address, save firewall logs to your local syslog daemon, and save firewall logs to a specified remote syslog server. See Configuring Log Settings, page 444.

STEP 3 Go to the **Device Management > Logs > Log Facilities** page to enable Email Alert, Local Log, and/or Remote Log for the firewall facility.

- To send firewall logs to a specified email address, check the box of Email Alert for the **Firewall** facility.
- To save firewall logs to the local syslog daemon, check the box of Local Log for the **Firewall** facility.
- To save firewall logs to the remote syslog server, check the box of Remote Log for the **Firewall** facility.

STEP 4 After you configure the firewall logging settings, go to the **Device Management > Logs > View Logs** page to view firewall logs. Choose **Firewall** from the Log Facility drop-down list to view firewall logs. You can filter firewall logs by the severity level or by the source and destination IP addresses. See Viewing Logs, page 442.

Configuring NAT Rules to Securely Access a Remote Network

Network Address Translation (NAT) enables private IP networks to connect to the Internet. NAT replaces a private IP address with a public IP address, translating the private addresses in the internal private network into legal, routable addresses that can be used on the public Internet. In this way, NAT conserves public addresses because it can be configured to advertise only one public address for the entire network to the outside world.

NAT can also provide the following benefits:

- **Security:** Keeping internal IP addresses hidden discourages direct attacks.
- **IP routing solutions:** Overlapping IP addresses are not a problem when you use NAT.
- **Flexibility:** You can change internal IP addressing schemes without affecting the public addresses available externally; for example, for a server accessible to the Internet, you can maintain a fixed IP address for Internet use, but internally, you can change the server address.

Refer to the following topics:

- Viewing NAT Translation Status, page 262
- Priorities of NAT Rules, page 263
- Configuring Dynamic PAT Rules, page 264
- Configuring Static NAT Rules, page 265
- Configuring Port Forwarding Rules, page 266
- Configuring Port Triggering Rules, page 268
- Configuring Advanced NAT Rules, page 269
- Configuring IP Alias for Advanced NAT rules, page 270
- Configuring an Advanced NAT Rule to Support NAT Hairpinning, page 272

NOTE For detailed NAT configuration examples, see Firewall and NAT Rule Configuration Examples, page 274.

Viewing NAT Translation Status

Use the NAT Status page to view information for all NAT rules. If one page cannot show all NAT entries, choose the page number from the drop-down list to view the NAT entries on another page.

Firewall > NAT > NAT Status

Field	Description
Original Source Address	Original source IP address in the packet.
Original Destination Address	Original destination IP address in the packet.
Source Port	Source interface that traffic comes from.
Destination Port	Destination interface that traffic goes to.
Translated Destination Address	IP address that the specified original destination address is translated to.

Field	Description
Translated Source Address	IP address that the specified original source address is translated to.
Translated Destination Port	Interface that the specified destination interface is translated to.
Translated Source Port	Interface that the specified source interface is translated to.
Tx Packets	Number of transmitted packets.
Rx Packets	Number of received packets.
Tx Bytes/Sec	Volume in bytes of transmitted traffic.
Rx Bytes/Sec	Volume in bytes of received traffic.

Priorities of NAT Rules

If there is a conflict between advanced NAT, static NAT, or port forwarding rules, the security appliance will process the rules as described below.

Inbound Traffic

For an inbound packet, the security appliance will perform NAT before a forwarding decision is made and will use the following order of precedence for the various types of rules:

1. Advanced NAT
2. Static NAT
3. Port Forwarding
4. Port Triggering

Outbound Traffic

For an outbound packet, the security appliance will perform NAT after a forwarding decision is made and will use the following order of precedence for various types of rules.

1. Advanced NAT
2. Static NAT
3. Dynamic PAT

For example, if an advanced NAT rule and a port forwarding rule conflict, then the advanced NAT rule will take precedence over the port forwarding rule and the port forwarding rule will not take effect.

Configuring Dynamic PAT Rules

Dynamic Port Address Translation (Dynamic PAT) can only be used to establish connections from private network to public network. Dynamic PAT translates multiple private addresses to one or more public IP address.

NOTE For the duration of the translation, a remote host can initiate a connection to the translated host if a firewall rule allows it. Because the port address (both real and mapped) is unpredictable, a connection to the host is unlikely. Nevertheless, in this case, you can rely on the security of the firewall rules.

STEP 1 Click **Firewall > NAT > Dynamic PAT**.

STEP 2 Specify the PAT IP address for each WAN port.

- **Auto:** Automatically use the IP address of the WAN port as the translated IP address.
- **Manual:** Manually choose a single public IP address or a network address as the translated IP address from the **IP Address** drop-down list. If the address object that you want is not in the list, choose **Create a new address** to create a new address object. To maintain the address objects, go to the **Networking > Address Management** page. See Address Management, page 175.

STEP 3 Translate multiple private IP addresses of a VLAN to one or more mapped IP addresses.

- **Enable WAN1:** Check this box to translate all IP addresses of the selected VLAN into the public IP address specified on the WAN1 port.
- **Enable WAN2:** Check this box to translate all IP addresses of the selected VLAN into the public IP address specified on the WAN2 port.
- **VLAN IP Address:** The subnet IP address and netmask of the selected VLAN.

STEP 4 Click **Save** to apply your settings.

Configuring Static NAT Rules

Static NAT creates a fixed translation of a real address to a mapped address. Because the mapped address is the same for each consecutive connection, static NAT allows bidirectional connection initiation, both to and from the host (if a firewall rule allows it). With dynamic PAT, on the other hand, each host uses a different address or port for each subsequent translation, so bidirectional initiation is not supported.

Up to 64 static NAT rules can be configured on the security appliance. You must create firewall rules to allow access so that the static NAT rules can function properly.

NOTE Remote management will not work if you configure a static NAT rule that maps an internal server to the WAN IP address. For example, if you create a static NAT rule that maps 192.168.75.100 to the WAN IP address, 173.39.202.68, then remote users will not have access to the configuration utility via http://173.39.202.68:8080.

STEP 1 Click **Firewall > NAT > Static NAT**.

STEP 2 To add a static NAT rule, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The Static NAT Rule - Add/Edit window opens.

STEP 3 Enter the following information:

- **WAN:** Choose either WAN1 or WAN2 as the WAN port.
- **Public IP:** Choose an IP address object as the public IP address.
- **Private IP:** Choose an IP address object as the private IP address.

  If the IP address that you want is not in the list, choose **Create a new address** to create a new IP address object. To maintain the IP address objects, go to the **Networking > Address Management** page. See Address Management, page 175.

  NOTE: Firewall rules must be configured to allow access. You can go to the **Firewall > Access Control > ACL Rules** page or click the **Create Rule** link to do this, but save your settings on this page first.

STEP 4 Click **OK** to save your settings.

STEP 5 Click **Save** to apply your settings.

Configuring Port Forwarding Rules

Port forwarding forwards a TCP/IP packet traversing a Network Address Translation (NAT) gateway to a pre-determined network port on a host within a NAT-masqueraded network, typically a private network based on the port number on which it was received at the gateway from the originating host.

Use the Port Forwarding page to assign a port number to a service that is associated with the application that you want to run, such as web servers, FTP servers, email servers, or other specialized Internet applications.

NOTE

- Up to 64 port forwarding rules can be configured on the security appliance. You must create firewall rules to allow access so that the port forwarding rules can function properly.
- To open an internal FTP server to the Internet, make sure that the FTP server is listening on TCP port 21 or both the FTP server and client must use the active mode when the FTP server is listening on some other TCP port. Otherwise the FTP client cannot access the FTP server.

STEP 1 Click **Firewall > NAT > Port Forwarding**.

STEP 2 To enable a port forwarding rule, check the box in the **Enable** column.

STEP 3 To add a port forwarding rule, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The Port Forwarding Rule - Add/Edit window opens.

STEP 4 Enter the following information:

- **Original Service:** Choose an existing service as the incoming service.
- **Translated Service:** Choose a service as the translated service or choose **Original** if the translated service is same as the incoming service. If the service that you want is not in the list, choose **Create a new service** to create a new service object. To maintain the service objects, go to the **Networking > Service Management** page. See Service Management, page 177.

NOTE: One-to-one translation will be performed for port range forwarding. For example, if you want to translate an original TCP service with the port range of 50000 to 50002 to a TCP service with the port range of 60000 to 60002, then the port 50000 will be translated to the port 60000, the port 50001 will be translated to the port 60001, and the port 50002 will be translated to the port 60002.

- **Translated IP:** Choose the IP address of your local server that needs to be translated. If the IP address that you want is not in the list, choose **Create a new address** to create a new IP address object. To maintain the IP address objects, go to the **Networking > Address Management** page. See Address Management, page 175.
- **WAN:** Choose either WAN1 or WAN2, or both as the incoming WAN port.
- **WAN IP:** Specify the public IP address of the server. You can use the IP address of the selected WAN port or a public IP address that is provided by your ISP. When you choose Both as the incoming WAN port, this option is grayed out.
- **Enable Port Forwarding:** Click **On** to enable the port forwarding rule, or click **Off** to create only the port forwarding rule.
- **Create Firewall Rule:** Check this box to automatically create a firewall rule to allow access so that the port forwarding rule can function properly. You must manually create a firewall rule if you uncheck this box.

  NOTE: If you choose Both as the incoming WAN port, a firewall rule from Any zone to Any zone will be created accordingly.
- **Description:** Enter the name for the port forwarding rule.

STEP 5 Click **OK** to save your settings.

STEP 6 Click **Save** to apply your settings.

Configuring Port Triggering Rules

Port triggering opens an incoming port for a specified type of traffic on a defined outgoing port. When a LAN device makes a connection on one of the defined outgoing ports, the security appliance opens the specified incoming port to support the exchange of data. The open ports will be closed again after 600 seconds when the data exchange is complete.

Port triggering is more flexible and secure than port forwarding, because the incoming ports are not open all the time. They are open only when a program is actively using the trigger port.

Some applications may require port triggering. Such applications require that, when external devices connect to them, they receive data on a specific port or range of ports in order to function properly. The security appliance must send all incoming data for that application only on the required port or range of ports. You can specify a port triggering rule by defining the type of traffic (TCP or UDP) and the range of incoming and outgoing ports to open when enabled.

NOTE Up to 15 port triggering rules can be configured on the security appliance. Port triggering is not appropriate for servers on the LAN, since the LAN device must make an outgoing connection before an incoming port is opened. In this case, you can create the port forwarding rules for this purpose.

STEP 1 Click **Firewall > NAT > Port Triggering**.

STEP 2 To enable a port triggering rule, check the box in the **Enable** column.

STEP 3 To add a new port triggering rule, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The Port Triggering Rule - Add/Edit window opens.

STEP 4 Enter the following information:

- **Description:** Enter the name for the port triggering rule.
- **Triggered Service:** Choose an outgoing TCP or UDP service.
- **Opened Service:** Choose an incoming TCP or UDP service.

  If the service that you want is not in the list, choose **Create a new service** to create a new service object. To maintain the service objects, go to the **Networking > Service Management** page. See Service Management, page 177.

- **Enable Port Triggering:** Click **On** to enable the port triggering rule, or click **Off** to create only the port triggering rule.

STEP 5 Click **OK** to save your settings.

STEP 6 Click **Save** to apply your settings.

Configuring Advanced NAT Rules

Advanced NAT allows you to identify real addresses and real ports for address translation by specifying the source and destination addresses.

NOTE Up to 32 advanced NAT rules can be configured on the security appliance. You must create firewall rules to allow access so that advanced NAT rules can function properly.

STEP 1 Click **Firewall > NAT > Advanced NAT**.

STEP 2 To enable an advanced NAT rule, check the box in the **Enable** column.

STEP 3 To add a new advanced NAT rule, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The Advanced NAT Rule - Add/Edit window opens.

STEP 4 Enter the following information:

- **Name:** Enter the name for the advanced NAT rule.
- **Enable:** Click **On** to enable the advanced NAT rule, or click **Off** to create only the advanced NAT rule.
- **From:** Choose **Any** or choose an interface (a WAN port or a VLAN) that traffic originates from.
- **To:** Choose **Any** or choose an interface (a VLAN or a WAN port) that traffic goes to.

  NOTE: When the original destination address is different with the translated destination address, you must choose **Any** for this option. When the original destination address is same with the translated destination address, you can choose a specific VLAN or WAN port for this option.

- **Original Source Address:** Choose the original source address for the packet.
- **Original Destination Address:** Choose the original destination address for the packet.
- **Original Services:** Choose the original TCP or UDP service.
- **Translated Source Address:** Choose the translated source address for the packet.
- **Translated Destination Address:** Choose the translated destination address for the packet.
- **Translated Services:** Choose the translated TCP or UDP service.

  If the address that you want is not in the list, choose **Create a new address** to create a new IP address object. To maintain the IP address objects, go to the **Networking > Address Management** page. See Address Management, page 175.

  If the service that you want is not in the list, choose **Create a new service** to create a new service object. To maintain the service objects, go to the **Networking > Service Management** page. See Service Management, page 177.

STEP 5 Click **OK** to save your settings.

STEP 6 Click **Save** to apply your settings.

STEP 7 Firewall rules must be configured to allow access so that advanced NAT rules can function properly. After you save your settings, go to the **Firewall > Access Control > ACL Rules** page to do this. See **Configuring a Firewall Rule, page 257**.

Configuring IP Alias for Advanced NAT rules

A single WAN port can be accessible through multiple IP addresses by adding an IP alias to the port. When you configure an advanced NAT rule, the security appliance will automatically create an IP alias in the following cases:

Use Case: The inbound interface (**From**) is set to a WAN port but the original destination IP address (**Original Destination Address**) is different with the public IP address of the selected WAN port.

For example, you host a HTTP server (192.168.75.20) on your LAN. Your ISP has provided a static IP address (1.1.1.3) that you want to expose to the public as your HTTP server address. You want to allow Internet user to access the internal HTTP server by using the specified public IP address.

Solution: Assuming that the IP address of the WAN1 port is 1.1.1.2 and you are assigned another public IP address 1.1.1.3. You can first create a host address object with the IP 192.168.75.20 called "HTTPServer" and a host address object with the IP 1.1.1.3 called "PublicIP", and then configure an advanced NAT rule as follows to open the HTTP server to the Internet.

From	WAN1 **NOTE:** It must be set as a WAN port and cannot be set as Any.
To	Any
Original Source Address	Any
Original Destination Address	PublicIP
Original Services	HTTP
Translated Source Address	Any
Translated Destination Address	HTTPServer
Translated Services	HTTP

Use Case: The outbound interface (**To**) is set to a WAN port but the translated source IP address (**Translated Source Address**) is different with the public IP address of the selected WAN port.

For example, you have provided a static IP address (1.1.1.3). The security appliance is set as a SSL VPN server. You want to translate the IP addresses of the SSL VPN clients to the specified public IP address when the SSL VPN clients access the Internet.

Solution: Assuming that the IP address of the WAN1 port is 1.1.1.2 and the SSL VPN client address pool is set as 192.168.200.0/24. You can first create a host address object with the IP 1.1.1.3 called "PublicIP," and then create an advanced NAT rule as follows to allow SSL VPN clients to access the Internet:

From	Any
To	WAN1 **NOTE:** It must be set as a WAN port and cannot be set as Any.
Original Source Address	SSLVPNPool
Original Destination Address	Any
Original Services	Any
Translated Source Address	PublicIP
Translated Destination Address	Any
Translated Services	Any

Configuring an Advanced NAT Rule to Support NAT Hairpinning

NAT hairpinning allows the hosts at LAN side to access internal servers by using their respective external IP addresses (public IP addresses). This section provides a configuration example about how to create an advanced NAT rule to support NAT hairpinning.

STEP 1 Go to the **Networking > Address Management** page to create a host address object with the IP 192.168.10.100 called "FTPServer." The FTP server locates in the LAN zone.

STEP 2 Go to the **Firewall > NAT > Port Forwarding** page to create a port forwarding rule as follows.

Original Service	FTP-CONTROL
Translated Service	FTP-CONTROL
Translated IP	FTPServer
WAN	WAN1
WAN IP	WAN1_IP
Enable Port Forwarding	On
Create Firewall Rule	On

STEP 3 A firewall rule will be automatically created as follows to allow access.

From Zone	WAN
To Zone	LAN
Services	FTP-CONTROL
Source Address	ANY
Destination Address	FTPServer
Match Action	Permit

STEP 4 Then go to the **Firewall > NAT > Advanced NAT** page to create an advanced NAT rule as follows.

From	DEFAULT
To	Any
Original Source Address	DEFAULT_NETWORK
Original Destination Address	WAN1_IP
Original Services	FTP-CONTROL

Translated Source Address	WAN1_IP
Translated Destination Address	FTPServer
Translated Services	FTP-CONTROL

Firewall and NAT Rule Configuration Examples

This section provides some configuration examples on adding firewall and NAT rules.

- **Allowing Inbound Traffic Using the WAN IP Address, page 274**
- **Allowing Inbound Traffic Using a Public IP Address, page 276**
- **Allowing Inbound Traffic from Specified Range of Outside Hosts, page 279**
- **Blocking Outbound Traffic by Schedule and IP Address Range, page 280**
- **Blocking Outbound Traffic to an Offsite Mail Server, page 280**

Allowing Inbound Traffic Using the WAN IP Address

Use Case: You host a FTP server on your LAN. You want to open the FTP server to Internet by using the IP address of the WAN1 port. Inbound traffic is addressed to your WAN1 IP address but is directed to the FTP server.

Solution: Perform the following tasks to complete the configuration:

STEP 1 Go to the **Networking > Address Management** page to create a host address object with the IP 192.168.75.100 called “InternalFTP.”

STEP 2 Go to the **Firewall > NAT > Port Forwarding** page to create a port forwarding rule as follows.

Original Service	FTP-CONTROL
Translated Service	FTP-CONTROL
Translated IP	InternalFTP
WAN	WAN1
WAN IP	WAN1_IP
Enable Port Forwarding	On

STEP 3 Or go to the **Firewall > NAT > Advanced NAT** page to create an advanced NAT rule as follows.

From	WAN1
To	DEFAULT
Original Source Address	ANY
Original Destination Address	WAN1_IP
Original Services	FTP-CONTROL
Translated Source Address	ANY
Translated Destination Address	InternalFTP
Translated Services	FTP-CONTROL

STEP 4 Then go to the **Firewall > Access Control > ACL Rules** page to create a firewall rule as follows to allow access:

From Zone	WAN
To Zone	LAN
Services	FTP-CONTROL

Source Address	ANY
Destination Address	InternalFTP
Match Action	Permit

NOTE When you create the port forwarding rule, you can check **Create Firewall Rule** to automatically generate the firewall rule.

Allowing Inbound Traffic Using a Public IP Address

Use Case: You host an RDP server on the DMZ. Your ISP has provided a static IP address that you want to expose to the public as your RDP server address. You want to allow Internet user to access the RDP server by using the specified public IP address.

Solution 1: Perform the following tasks to complete the configuration:

STEP 1 Go to the Networking > Address Management page to create a host address object with the IP 192.168.12.101 called “RDPServer” and a host address object with the IP 172.39.202.102 called “PublicIP.”

STEP 2 Go to the Networking > Service Management page to create a TCP service object with the port 3389 called “RDP.”

STEP 3 Go to the Firewall > NAT > Port Forwarding page to create a port forwarding rule as follows.

Original Service	RDP
Translated Service	RDP
Translated IP	RDPServer
WAN	WAN1
WAN IP	PublicIP
Enable Port Forwarding	On
Create Firewall Rule	On

STEP 4 Or go to the Firewall > NAT > Advanced NAT page to create an advanced NAT rule as follows.

From	WAN1
To	DMZ
Original Source Address	ANY
Original Destination Address	PublicIP
Original Services	RDP
Translated Source Address	ANY
Translated Destination Address	RDPServer
Translated Services	RDP

STEP 5 Then go to the Firewall > Access Control > ACL Rules page to create a firewall rule as follows to allow access:

From Zone	WAN
To Zone	DMZ
Services	RDP
Source Address	ANY
Destination Address	RDPServer
Match Action	Permit

NOTE When you create the port forwarding rule, you can check **Create Firewall Rule** to automatically generate the firewall rule.

Solution 2: For this use case, you can use the DMZ Wizard to complete the configuration.

STEP 1 Click **Configuration Wizards > DMZ Wizard**.

STEP 2 In the DMZ Configuration page, configure a DMZ network as follows:

Name	DMZ
IP	192.168.12.1
Netmask	255.255.255.0
Port	GE6
Zone	DMZ

STEP 3 In the DMZ Service page, create a DMZ service as follows:

Original Service	RDP
Translated Service	RDP
Translated IP	RDPServer
WAN	WAN1
WAN IP	PublicIP
Enable DMZ Service	On
Create Firewall Rule	On

STEP 4 Click **Finish** to apply your settings.

STEP 5 A firewall rule will be automatically generated as follows to allow access.

From Zone	WAN
To Zone	DMZ
Services	RDP
Source Address	ANY
Destination Address	RDPServer

Match Action	Permit

Allowing Inbound Traffic from Specified Range of Outside Hosts

Use Case: You want to allow incoming video conferencing to be initiated from a restricted range of outside IP addresses (132.177.88.2 to 132.177.88.254). In the example, connections for CU-SeeMe (an Internet video-conferencing client) are allowed only from a specified range of external IP addresses.

Solution: Perform the following tasks to complete the configuration:

STEP 1 Go to the Networking > Address Management page to create an address object with the range 132.177.88.2 to 132.177.88.254 called "OutsideNetwork" and a host address object with the IP 192.168.75.110 called "InternalIP."

STEP 2 Go to the Firewall > NAT > Port Forwarding page to create a port forwarding rule as follows.

Original Service	CU-SEEME
Translated Service	CU-SEEME
Translated IP	InternalIP
WAN	WAN1
WAN IP	WAN1_IP
Enable Port Forwarding	On
Create Firewall Rule	Off

STEP 3 Go to the Firewall > Access Control > ACL Rules page and create the ACL rule as described below.

From Zone	WAN
To Zone	LAN

Services	CU-SEEME
Source Address	OutsideNetwork
Destination Address	InternalIP
Match Action	Permit

Blocking Outbound Traffic by Schedule and IP Address Range

Use Case: Block all weekend Internet usage if the request originates from a specified range of IP addresses.

Solution: Create an address object with the range 10.1.1.1 to 10.1.1.100 called "TempNetwork" and a schedule called "Weekend" to define the time period when the firewall rule is in effect. Then create a firewall rule as follows:

From Zone	LAN
To Zone	WAN
Services	HTTP
Source Address	TempNetwork
Destination Address	Any
Schedule	Weekend
Match Action	Deny

Blocking Outbound Traffic to an Offsite Mail Server

Use Case: Block access to the SMTP service to prevent a user from sending email through an offsite mail server.

Solution: Create a host address object with the IP address 10.64.173.20 called "OffsiteMail" and then create a firewall rule as follows:

From Zone	LAN
To Zone	WAN
Services	SMTP
Source Address	Any
Destination Address	OffsiteMail
Match Action	Deny

Configuring Content Filtering to Control Internet Access

Content Filtering blocks or allows HTTP access to websites containing specific keywords or domains. It controls access to certain Internet sites based on analysis of its content (domain or URL keyword), rather than its source or other criteria. It is most widely used on the Internet to filter web access.

Refer to the following topics:

- **Configuring Content Filtering Policy Profiles, page 281**
- **Configuring Website Access Control List, page 282**
- **Mapping Content Filtering Policy Profiles to Zones, page 283**
- **Configuring Advanced Content Filtering Settings, page 284**

NOTE Enabling Firewall Content Filtering will disable Web URL Filtering. Enabling Web URL Filtering will disable Firewall Content Filtering.

Configuring Content Filtering Policy Profiles

A content filtering policy profile is used to specify which websites are blocked or allowed.

NOTE Up to 16 content filtering policy profiles can be configured on the security appliance.

STEP 1 Click **Firewall > Content Filtering > Content Filtering Policies**.

STEP 2 To add a content filtering policy profile, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon.

The Content Filtering Policies - Add/Edit window opens.

STEP 3 Enter the following information:

- **Policy Profile:** Enter the name for the content filtering policy profile.
- **Description:** Enter a brief description for the content filtering policy profile.

STEP 4 In the **Website Access Control List** area, specify the list of websites that you want to allow or block. See **Configuring Website Access Control List, page 282**.

STEP 5 In the **For URLs not specified above** area, specify how to deal with the websites that are not specified in the list.

- **Permit them:** If you choose this option, all websites not specified in the list are allowed.
- **Deny them:** If you choose this option, all websites not specified in the list are blocked.

STEP 6 Click **OK** to save your settings.

STEP 7 Click **Save** to apply your settings.

Configuring Website Access Control List

This section describes how to specify the website access control list to control access for specific websites.

NOTE Up to 32 website access rules can be configured for each content filtering policy profile.

STEP 1 In the **Website Access Control List** area, click **Add** to add a website access rule.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete all entries, click **Delete All**.

The Website Access Control List - Add/Edit window opens.

STEP 2 Enter the following information:

- **Enable Content Filter URL:** Click **On** to enable the website access rule, or click **Off** to create only the website access rule.
- **URL:** Enter the domain name or URL keyword of a website that you want to permit or block.
- **Match Type:** Specify how to match this rule:
  - **Web Site:** If you choose this option, permit or block the HTTP access of a website that fully matches the domain that you entered in the **URL** field.

    For example, if you enter yahoo.com in the URL field, then it can match the website http://yahoo.com/*, but cannot match the website http://*.yahoo.com.uk/*.
  - **URL Keyword:** If you choose this option, permit or block the HTTP access of a website that contains the keyword that you entered in the **URL** field.

    For example, if you enter yahoo in the URL field, then it can match the websites such as www.yahoo.com, tw.yahoo.com, www.yahoo.com.uk, and www.yahoo.co.jp.
- **Action:** Choose **Permit** to permit access, or choose **Block** to block access.

STEP 3 Click **OK** to save your settings.

Mapping Content Filtering Policy Profiles to Zones

Use the Policy to Zone Mapping page to apply the content filtering policy profile to each zone. The content filtering policy profile assigned to each zone determines whether to block or forward the HTTP requests from the hosts in the zone. The blocked requests will be logged.

STEP 1 Click **Firewall > Content Filtering > Policy to Zone Mapping**.

The Policy to Zone Mapping window opens.

STEP 2 Click **On** to enable the Content Filtering feature, or click **Off** to disable it.

STEP 3 Specify the policy profile for each zone. By default, the Default_Profile that permits all websites is selected for all predefined and new zones.

STEP 4 Click **Save** to apply your settings.

Configuring Advanced Content Filtering Settings

STEP 1 Click **Firewall > Content Filtering > Advanced Settings**.

STEP 2 Enter the following information:

- **Filter Traffic on HTTP Port:** Enter the port number that is used for filtering HTTP traffic. Content Filtering only monitors and controls the website visits through this HTTP port. The default value is 80.
- **Filter Traffic on HTTPS port:** Enter the port number that is used for filtering HTTPS traffic. Web URL Filtering only monitors and controls the website visits through this HTTPS port. The default value is 443.
- **Blocked Web Components:** You can block web components like Proxy, Java, ActiveX, and Cookies. By default, all of them are permitted.
  - **Proxy:** Check this box to block proxy servers, which can be used to circumvent certain firewall rules and thus present a potential security gap.
  - **Java:** Check this box to block Java applets that can be downloaded from pages that contain them.
  - **ActiveX:** Check this box to prevent ActiveX applets from being downloaded through Internet Explorer.
  - **Cookies:** Check this box to block cookies, which typically contain sessions.
- **Action:** Choose one of the following actions when a web page is blocked:
  - **Display Default Blocked Page when the requested page is blocked:** Displays the default block page if a web page is blocked. If you choose this option, the message that you specify in the **Block Message** field will show on the default block page.
  - **Redirect URL:** Redirects to a specified web page if a web page is blocked. If you choose this option, enter a desired URL to be redirected. Make sure that specified URL is allowed by the Website Access Control List.

STEP 3 Click **Save** to apply your settings.

Configuring MAC Address Filtering to Permit or Block Traffic

MAC Address Filtering permits and blocks network access from specific devices through the use of MAC address list. The MAC Address Filtering settings apply for all traffic except Intra-VLAN and Intra-SSID.

STEP 1 Click **Firewall > MAC Filtering > MAC Address Filtering**.

The MAC Address Filtering window opens.

STEP 2 Click **On** to enable the MAC Address Filtering feature, or click **Off** to disable it.

STEP 3 If you enable MAC Address Filtering, choose one of the following options as the MAC Address Filtering policy:

- **Block MAC Addresses (and allow all others):** The MAC addresses in the list are blocked and all other MAC addresses not included in the list are permitted.
- **Allow MAC Addresses (and block all others):** Only the MAC addresses in the list are permitted and all other MAC addresses not included in the list are blocked.

STEP 4 In the **MAC Address Filtering Rules** area, specify the list of MAC addresses. To add a MAC address, click **Add**. To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

For example, if you click **Add**, the MAC Address Filtering Rule - Add/Edit window opens. Choose the MAC address object from the **MAC Address** drop-down list and click **OK**. If the MAC address object that you want is not in the list, choose **Create a new address** to create a new MAC address object. To maintain the MAC address objects, go to the Networking > Address Management page. See Address Management, page 175.

STEP 5 Click **Save** to apply your settings.

Configuring IP-MAC Binding to Prevent Spoofing

IP-MAC Binding allows you to bind an IP address to a MAC address and vice-versa. It only allows traffic when the host IP address matches a specified MAC address. By requiring the gateway to validate the source traffic's IP address with the unique MAC address of device, this ensures that traffic from the specified IP address is not spoofed. If a violation (the traffic's source IP address doesn't match the expected MAC address having the same IP address), the packets will be dropped and can be logged for diagnosis.

NOTE Up to 100 IP-MAC binding rules can be configured on the security appliance.

STEP 1 Click **Firewall > MAC Filtering > IP - MAC Binding Rules**.

The IP - MAC Binding Rules window opens.

STEP 2 To add an IP-MAC binding rule, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The IP&MAC Binding Rule - Add/Edit window opens.

STEP 3 Enter the following information:

- **Name:** Enter the name for the IP-MAC binding rule.
- **MAC Address:** Choose an existing MAC address object. If the MAC address object that you want is not in the list, choose **Create a new address** to add a new MAC address object. To maintain the MAC address objects, go to the Networking > Address Management page. See Address Management, page 175.
- **IP Address:** Choose an existing IP address object that you want to bind with the selected MAC address. If the IP address object that you want is not in the list, choose **Create a new address** to add a new IP address object. To maintain the IP address objects, go to the Networking > Address Management page. See Address Management, page 175.
- **Log Dropped Packets:** Choose **Enable** to log all packets that are dropped. Otherwise, choose **Disable**.

STEP 4 Click **OK** to save your settings.

STEP 5 Click **Save** to apply your settings.

Configuring Attack Protection

Use the Attack Protection page to specify how to protect your network against common types of attacks including discovery, flooding, and echo storms.

STEP 1 Click **Firewall > Attack Protection**.

STEP 2 In the **WAN Security Checks** area, enter the following information:

- **Block Ping WAN Interface:** Check this box to prevent attackers from discovering your network through ICMP Echo (ping) requests. We recommend that you disable this feature only if you need to allow the security appliance to respond to pings for diagnostic purposes.
- **Stealth Mode:** Check this box to prevent the security appliance from responding to incoming connection requests from the WAN ports. In Stealth Mode, the security appliance does not respond to blocked inbound connection requests, and your network is less susceptible to discovery and attacks.
- **Block TCP Flood:** Check this box to drop all invalid TCP packets. This feature protects your network from a SYN flood attack, in which an attacker sends a succession of SYN (synchronize) requests to a target system. It blocks all TCP SYN flood attacks (more than 200 simultaneous TCP packets per second) from the WAN ports.

STEP 3 In the **LAN Security Checks** section, enter the following information:

- **Block UDP Flood:** Check this box to limit the number of simultaneous, active UDP connections from a single computer on the LAN. If you enable this feature, also enter the number of connections to allow per host per second. The default value is 500, and the valid range is from 100 to 10,000. When this limit is reached, the security appliance considers it a UDP flood attack and drops all connections from the host.

STEP 4 In the **Firewall Settings** area, enter the following information:

- **Block ICMP Notification:** Check this box to silently block without sending an ICMP notification to the sender. Some protocols, such as MTU Path Discovery, require ICMP notifications.
- **Block Fragmented Packets:** Check this box to block fragmented packets from Any zone to Any zone.

- **Block Multicast Packets:** Check this box to block multicast packets. By default, the firewall blocks all multicast packets. This feature has higher priority than the firewall rules, which indicates that the firewall rules that permit multicast traffic will be overridden if you enable this feature.

STEP 5 In the **DoS Attacks** area, enter the following information:

- **SYN Flood Detect Rate:** Enter the maximum number of SYN packets per second that will cause the security appliance to determine that a SYN Flood Intrusion is occurring. Enter a value from 0 to 65535 SYN packets per second. The default value is 128 SYN packets per seconds. A value of zero (0) indicates that the SYN Flood Detect feature is disabled.
- **Echo Storm:** Enter the number of pings per second that will cause the security appliance to determine that an echo storm intrusion event is occurring. Enter a value from 0 to 65535 ping packets per second. The default value is 15 ping packets per seconds. A value of zero (0) indicates that the Echo Storm feature is disabled.
- **ICMP Flood:** Enter the number of ICMP packets per second, including PING packets, that will cause the security appliance to determine that an ICMP flood intrusion event is occurring. Enter a value from 0 to 65535 ICMP packets per second. The default value is 100 ICMP packets per seconds. A value of zero (0) indicates that the ICMP Flood feature is disabled.

  NOTE: When one of DoS attack levels is exceeded, that kind of traffic will be dropped.

STEP 6 Click **Save** to apply your settings.

Configuring Session Limits

Use the Session Limits page to configure the maximum number of connection sessions. When the connection table is full, the new sessions that access the security appliance are dropped.

STEP 1 Click **Firewall > Session Limits**.

STEP 2 Enter the following information:

- **Current All Connections:** Displays the total number of current connections. Click **Disconnect All** to clean up all connected sessions.

- **Maximum Connections:** Limit the number for TCP and UDP connections. Enter a value in the range 1000 to 60000. The default value is 60000.
- **TCP Timeout:** Enter the timeout value in seconds for TCP session. Inactive TCP sessions are removed from the session table after this duration. The valid range is 5 to 3600 seconds. The default value is 1200 seconds.
- **UDP Timeout:** Enter the timeout value in seconds for UDP session. Inactive UDP sessions are removed from the session table after this duration. The valid range is 5 to 3600 seconds. The default value is 180 seconds.

STEP 3 Click **Save** to apply your settings.

Configuring Application Level Gateway

The security appliance can function as an Application Level Gateway (ALG) to allow certain NAT incompatible applications (such as SIP or H.323) to operate properly through the security appliance.

If Voice-over-IP (VoIP) is used in your organization, you should enable H.323 ALG or SIP ALG to open the ports necessary to allow the VoIP through your voice device. The ALGs are created to work in a NAT environment to maintain the security for privately addressed conferencing equipment protected by your voice device.

You can use both H.323 ALG and SIP ALG at the same time, if necessary. To determine which ALG to use, consult the documentation for your VoIP devices or applications.

STEP 1 Click **Firewall > Application Level Gateway**.

The Application Level Gateway window opens.

STEP 2 Enter the following information:

- **SIP Support:** SIP ALG can rewrite the information within the SIP messages (SIP headers and SDP body) to make signaling and audio traffic between the client behind NAT and the SIP endpoint possible. Check this box to enable SIP ALG support, or uncheck this box to disable this feature.

  NOTE: Enable SIP ALG when voice devices such as UC500, UC300, or SIP phones are connected to the network behind the security appliance.

- **H.323 Support:** H.323 is a standard teleconferencing protocol suite that provides audio, data, and video conferencing. It allows for real-time point-to-point and multipoint communication between client computers over a packet-based network that does not provide a guaranteed quality of service. Check this box to enable H.323 ALG support, or uncheck this box to disable this feature.
- **FTP Support on TCP port:** Check the box to enable FTP support, or uncheck the box to disable the this feature. Then choose a listening port. The default port is FTP-CONTROL (21).

STEP 3 Click **Save** to apply your settings.

7

Security Services

This chapter describes how to configure Unified Threat Management (UTM) security services to provide protection from Internet threats. It includes the following sections:

- About Security Services, page 292
- Activating Security Services, page 293
- Priority of Security Services, page 293
- Security Services Dashboard, page 294
- Viewing Security Services Reports, page 295
- Configuring Anti-Virus, page 302
- Configuring Application Control, page 309
- Configuring Spam Filter, page 319
- Configuring Intrusion Prevention, page 321
- Configuring Web Reputation Filtering, page 325
- Configuring Web URL Filtering, page 327
- Network Reputation, page 332

To access the Security Services pages, click **Security Services** in the left hand navigation pane.

About Security Services

The security appliance supports a variety of UTM security services to provide the Internet threat protection for your network. By default, all security services except Network Reputation are disabled.

The following table lists all available security services on the security appliance.

Security Service	Description
Anti-Virus	Anti-Virus prevents network threats over a multitude of protocols, including HTTP, FTP, POP3, SMTP, CIFS, NETBIOS, and IMAP. See **Configuring Anti-Virus, page 302**.
Application Control	Application Control monitors and controls the use of applications on your network. See **Configuring Application Control, page 309**.
Spam Filter	Spam Filter detects the email sender's reputation score. If the reputation score is below the threshold, then the email is blocked or tagged as spam or suspected spam. See **Configuring Spam Filter, page 319**.
Intrusion Prevention (IPS)	IPS monitors network traffic for malicious or unwanted behaviors and can react, in real-time, to block or prevent those activities. See **Configuring Intrusion Prevention, page 321**.
Network Reputation	Network Reputation blocks incoming traffic from IP addresses that are known to initiate attacks throughout the Internet. See **Network Reputation, page 332**.
Web Reputation Filtering	Web Reputation Filtering prevents client devices from accessing dangerous websites containing viruses, spyware, malware, or phishing links. See **Configuring Web Reputation Filtering, page 325**.
Web URL Filtering	Web URL Filtering allows you to block HTTP access to malicious websites based on URL categories. See **Configuring Web URL Filtering, page 327**.

Anti-Virus, Application Control, and IPS are signature-based security services. You must update the signatures frequently to ensure that these security services can give you the best protection.

Spam Filter, Network Reputation, Web Reputation Filtering, and Web URL Filtering are reputation-based security services. They obtain the security data from the SecApps servers and determine which traffic is allowed or blocked. Make sure that the SecApps servers are online after you enable these security services, otherwise they will not be available.

Activating Security Services

The security services are licensable. You must install a valid security license on the security appliance to activate security services. A valid security license is also required for support of SSLVPN with mobile devices such as smart phones and tablets.The Product Authorization Key (PAK) is required to validate the security license. You can find the license code from the Software License Claim Certificate that Cisco provides upon purchase of the security appliance.

Make sure that the security license is installed and does not expire before you configure security services. Go to the Device Management > License Management page to validate the security license or to renew the security license before it expires. See Installing or Renewing Security License, page 441.

Priority of Security Services

Multiple security services can work simultaneously to protect your network. Web Reputation Filtering has a higher priority than Web URL Filtering. You can add the website exceptions in the website access control list when you configure a Web URL Filtering policy profile. The website exceptions can override the profile's URL category settings, but cannot override the Web Reputation Filtering settings.

For example, a website as an exception is allowed to access by Web URL Filtering, but it has reputation score lower than the web reputation threshold specified in Web Reputation Filtering. Web Reputation Filtering will block access to this website even if it is an exception in the website access control list, unless you change the web reputation threshold.

Security Services Dashboard

Use the Dashboard page to view the status of the security license, enable or disable security services, and check for signature updates for all signature-based security services.

STEP 1 Click **Security Services > Dashboard**.

The Dashboard window opens.

STEP 2 In the **License Status** area, the security license status is displayed. If the security license expires, go to the Device Management > License Management page to renew the license. See Installing or Renewing Security License, page 441.

STEP 3 In the **Settings Summary** area, you can perform the following tasks:

- To enable a security service, check the box in the **Enable** column. By default, only Network Reputation is enabled.
- To configure the settings for a security service, click **Configure**.
- To immediately check for new updates for security services, click **Check for Updates Now**.
  - For signature-based security services such as Anti-Virus, Application Control, and IPS, clicking this button will check for signature updates from Cisco's signature server. Anti-Virus and IPS use different signature database but IPS and Application Control use the same signature database. This operation will check for signature updates for all of them at a time. If a newer signature file than your current one is available on the server, the new signature file will be downloaded to your device.

    NOTE: A valid Cisco.com account is required to check for signature updates from Cisco's signature server. Go to the Device Management > Cisco.com Account page to configure your Cisco.com account credentials on the security appliance. See Configuring Cisco.com Account, page 424.
  - For reputation-based security services such as Spam Filter, Web URL Filtering, Web Reputation Filtering, and Network Reputation, clicking this button will only check for new updates for Network Reputation. This operation will not check for new updates for Spam Filter, Web URL Filtering, and Web Reputation Filtering.

The date and time of your last check are displayed in the **Last Check** column. When a signature file is updated successfully, the date and time of the last successful update are displayed in the **Last Update** column.

- Spam Filter, Web URL Filtering, Web Reputation Filtering, and Network Reputation obtain the security data from the SecApps servers and determine which traffic is allowed or blocked. The **Server Status** column displays the status of SecApps servers. Make sure that the SecApps servers are online after you enable these security services; otherwise they will not be available.

STEP 4 In the **External Web Proxy Settings** area, specify an external web proxy used to redirect HTTP traffic if needed:

- **External Web Proxy:** Click **On** to support such as Scansafe and third party outbound web proxies, or click **Off** to disable it.

  NOTE: When the external web proxy feature is enabled, the Firewall, QoS, Web URL Filtering, and Web Reputation Filtering settings will not work or be skipped for HTTP traffic.

- **Redirected Web Proxy IP Address:** Enter the IP address of the external web proxy used to redirect HTTP traffic.

- **Redirected HTTP Ports:** Specify the proxy ports. To add an entry, click **Add**. To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon.

STEP 5 Click **Save** to apply your settings.

Viewing Security Services Reports

Use the Security Services Reports page to view the reports for all security services. To open the page, click **Security Services > Security Services Reports**. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data. Refer to the following topics:

- **Viewing Web Security Report, page 296**
- **Viewing Anti-Virus Report, page 297**
- **Viewing Email Security Report, page 298**
- **Viewing Network Reputation Report, page 299**

- Viewing IPS Report, page 300
- Viewing Application Control Report, page 301

NOTE The security services reports are only active after the security license is installed. Before you choose a report to view, make sure that the corresponding security service is enabled.

Viewing Web Security Report

This report displays the number of web access requests logged and the number of websites blocked by Web URL Filtering, Web Reputation Filtering, or both.

STEP 1 In the **Web Security** tab, specify the following information:

- **Enable:** Check this box to enable the web security report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of websites blocked by Web URL Filtering and/or Web Reputation Filtering in the graph. To view more information about blocked requests, click the red bar in the graph. A pop-up window displays the following information for each blocked request: the date and the time, the IP address and the MAC address of the host that initiated the request, the web site, the blocked URL, the filter that blocked the request, and the number of times that the connection was blocked.
- **Processed Requests:** Check this box to display the number of web access requests logged by Web URL Filtering and/or Web Reputation Filtering in the graph.

STEP 2 Click **Save** to apply your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of web access requests processed and total number of websites blocked since Web URL Filtering and Web Reputation Filtering were activated.

Field	Description
Total Last 7 Days	Total number of web access requests processed and total number of websites blocked in last seven days.
Total Today	Total number of web access requests processed and total number of websites blocked in one day.
Graph	Total number of web access requests processed and total number of websites blocked per day in last seven days.

Viewing Anti-Virus Report

This report displays the number of files checked and the number of viruses detected by the Anti-Virus service.

STEP 1 In the **Anti-Virus** tab, specify the following information:

- **Enable:** Check this box to enable the Anti-Virus report, or uncheck this box to disable it.
- **Detected Requests:** Check this box to display the number of viruses detected by the Anti-Virus service in the graph. To view more information about detected requests, click the red bar in the graph. A pop-up window displays the following information for each detected request: the date and the time, the IP address and the MAC address of the source and of the destination, the protocol used for the connection, the action taken, and the number of times a virus was found.
- **Processed Requests:** Check this box to display the number of files checked by the Anti-Virus service in the graph.

STEP 2 Click **Save** to apply your settings.

Field	Description
System Date	Current system time.

Field	Description
Total Since Activated	Total number of files checked and total number of viruses detected since the Anti-Virus service was activated.
Total Last 7 Days	Total number of files checked and total number of viruses detected in last seven days.
Total Today	Total number of files checked and total number of viruses detected in one day.
Graph	Total number of files checked and total number of viruses detected per day in last seven days.

Viewing Email Security Report

This report displays the number of emails checked and the number of spam or suspected spam emails detected by the Spam Filter service.

STEP 1 In the **Email Security** tab, specify the following information:

- **Enable:** Check this box to enable the email security report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of spam or suspected spam emails detected by the Spam Filter service in the graph.
- **Processed Requests:** Check this box to display the number of emails checked by the Spam Filter service in the graph.

STEP 2 Click **Save** to apply your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of emails checked and total number of spam or suspected spam emails detected since the Spam Filter service was activated.

Field	Description
Total Last 7 Days	Total number of emails checked and total number of spam or suspected spam emails detected in last seven days.
Total Today	Total number of emails checked and total number of spam or suspected spam emails detected in one day.
Graph	Total number of emails checked and total number of spam or suspected spam emails detected per day in last seven days.

Viewing Network Reputation Report

This report displays the number of packets checked and the number of packets blocked by the Network Reputation service.

STEP 1 In the **Network Reputation** tab, specify the following information:

- **Enable:** Check this box to enable the network reputation report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of packets blocked by the Network Reputation service in the graph.
- **Processed Requests:** Check this box to display the number of packets checked by the Network Reputation service in the graph.

STEP 2 Click **Save** to apply your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of packets checked and total number of packets blocked since the Network Reputation service was activated.
Total Last 7 Days	Total number of packets checked and total number of packets blocked in last seven days.

Field	Description
Total Today	Total number of packets checked and total number of packets blocked in one day.
Graph	Total number of packets checked and total number of packets blocked per day in last seven days.

Viewing IPS Report

This report displays the number of packets detected and the number of packets dropped by the IPS service.

STEP 1 In the **IPS** tab, specify the following information:

- **Enable:** Check this box to enable the IPS report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of packets dropped by the IPS service in the graph. To view more information about blocked requests, click the red bar in the graph. A pop-up window displays the following information for each blocked request: the date and time, the IP address and the MAC address of the source and of the destination, the action taken, and the number of times that this event was detected.
- **Processed Requests:** Check this box to display the number of packets detected by the IPS service in the graph.

STEP 2 Click **Save** to apply your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of packets detected and total number of packets dropped since the IPS service was activated.
Total Last 7 Days	Total number of packets detected and total number of packets dropped in last seven days.
Total Today	Total number of packets detected and total number of packets dropped in one day.

Field	Description
Graph	Total number of packets detected and total number of packets dropped per day in last seven days.

Viewing Application Control Report

This report displays the number of packets detected and the number of packets blocked by the Application Control service.

STEP 1 In the **Application Control** tab, specify the following information:

- **Enable:** Check this box to enable the application control report, or uncheck this box to disable it.
- **Blocked Requests:** Check this box to display the number of packets dropped by the Application Control service in the graph. To view more information about blocked requests, click the red bar in the graph. A pop-up window displays the following information for each blocked request: the date and time, the IP address and the MAC address of the host that initiated the request, the blocked application, and the number of times that the application was blocked.
- **Processed Requests:** Check this box to display the number of packets detected by the Application Control service in the graph.

STEP 2 Click **Save** to apply your settings.

Field	Description
System Date	Current system time.
Total Since Activated	Total number of packets detected and total number of packets blocked since the Application Control service was activated.
Total Last 7 Days	Total number of packets detected and total number of packets blocked in last seven days.
Total Today	Total number of packets detected and total number of packets blocked in one day.

Field	Description
Graph	Total number of packets detected and total number of packets blocked per day in last seven days.

Configuring Anti-Virus

Anti-Virus helps protect your network from viruses and malware. Anti-Virus scans for viruses over a multitude of protocols, including HTTP, FTP, POP3, SMTP, CIFS, NETBIOS, and IMAP.

NOTE Anti-Virus covers the most recent and widespread threats but cannot detect all known viruses (including rare samples). It delivers "first layer defense," efficiently handles malware outbreaks, and catches the most widespread and the most dangerous malware (commonly known as "in-the-wild" malware). Currently, the most widespread types of malware are worms, trojans, exploits, viruses, and rootkits. As new, widespread threats emerge, Anti-Virus will expand to include the most dangerous types of threats.

You can apply the Anti-Virus service to the zones. Anti-Virus examines all incoming and outgoing traffic for the selected zones and performs the action that you specify for different types of traffic. You can choose to drop the connection, delete the infected files, and/or send an alert email to the email receiver if viruses are detected.

Because files containing malicious code and viruses can be compressed, Anti-Virus can automatically decompress the compressed files and then scan the viruses. Anti-Virus supports scanning single level compressed files for these file types: zip, gzip, tar, rar 2.0, and bz2 (Bzip).

Anti-Virus uses signatures to identify the infected files. You must update the signatures frequently to keep the protection current. See **Updating Anti-Virus Signatures, page 308**.

You can enable the Anti-Virus report from the Security Services > Security Services Reports page or from the Status > Security Services Reports page to see the number of files checked and the number of viruses detected by the Anti-Virus service. See **Viewing Anti-Virus Report, page 297**.

You can enable the Anti-Virus Alert feature to send an alert email for virus events at a specified interval to a specified email address. See Configuring Email Alert Settings, page 408.

Refer to the following topics:

- General Anti-Virus Settings, page 303
- Configuring Advanced Anti-Virus Settings
- Configuring HTTP Notification, page 307
- Configuring Email Notification, page 307
- Updating Anti-Virus Signatures, page 308

General Anti-Virus Settings

Use the General Settings page to enable or disable Anti-Virus, specify the zones to scan for viruses, and configure the preventive actions for different types of traffic, and set the maximum file size to scan.

STEP 1 Click **Security Services > Anti-Virus > General Settings**.

STEP 2 Click **On** to enable Anti-Virus, or click **Off** to disable it.

STEP 3 In the **Zone to Scan** area, specify the zones to scan the viruses:

- **WAN Zone:** Choose this option to scan the viruses for all incoming and outgoing traffic for the WAN zone.
- **WAN+VPN Zone:** Choose this option to scan the viruses for all incoming and outgoing traffic for both WAN and VPN zones.
- **All Zone:** Choose this option to scan the viruses for all incoming and outgoing traffic for all zones.

STEP 4 In the **Applications to Scan** area, perform the following tasks to scan for viruses on your network:

- **Enable:** Check the box in this column to scan for viruses over a protocol.
- **Logging:** Check the box in this column to log the events when viruses are detected.

  To log Anti-Virus events, you must first check the **Logging** box for the protocols, and then go to the Device Management > Logs pages to configure the log settings and log facilities. See Log Management, page 442.

  - To save Anti-Virus logs to the local syslog daemon, you must enable the Log feature, set the log buffer size and the severity level for local logs, and then enable the Local Log settings for the Anti-Virus facility.

- To save Anti-Virus logs to the remote syslog server if you have a remote syslog server support, you must enable the Log feature, specify the Remote Log settings, and enable the Remote Log settings for the Anti-Virus facility.

- **Action:** Specify the preventive action for different types of traffic when viruses are detected. The following table lists all available actions for each protocol.

Protocol	Action
HTTP	**None:** No action is required when viruses are detected. **Notify:** Send an alert message to the user when viruses are detected in web pages or in files that the user tries to access. **Notify + Drop Connection:** Drop the connection and send an alert message to the user when viruses are detected in web pages or in files that the user tries to access. **Disable HTTP Resume:** Optionally, check this box to disable resuming web-based file transfer by using the HTTP protocol when viruses are detected. **NOTE:** If you choose Notify or Notify + Drop Connection, go to the HTTP Notification page to configure the notification message. See **Configuring HTTP Notification, page 307**.
FTP	**None:** No action is required when viruses are detected. **Drop Connection:** Drop the connection when viruses are detected. **Disable FTP Resume:** Optionally, check this box to disable resuming file transfer by using the FTP protocol when viruses are detected.

Protocol	Action
SMTP Email Attachments	**None:** No action is required when viruses are detected. **Notify:** Send the original email and an alert email to the email receiver when viruses are detected in email attachments. **Notify + Destruct File:** Delete the infected files and send the original email and an alert email to the email receiver when viruses are detected in email attachments. **NOTE:** If you choose Notify or Notify + Destruct File, go to the Email Notification page to configure the email notification settings. See **Configuring Email Notification, page 307**.
POP3 Email Attachments	**None:** No action is required when viruses are detected. **Notify:** Send the original email and an alert email to the email receiver when viruses are detected in email attachments. **Notify + Destruct File:** Delete the infected files and send the original email and an alert email to the email receiver when viruses are detected in email attachments. **NOTE:** If you choose Notify or Notify + Destruct File, go to the Email Notification page to configure the email notification settings. See **Configuring Email Notification, page 307**.
IMAP Email Attachments	**None:** No action is required when viruses are detected. **Destruct File:** Delete the infected files when viruses are detected in email attachments.
NETBIOS/ CIFS	**None:** No action is required when viruses are detected. **Drop Connection:** Drop the connection when viruses are detected.

STEP 5 In the **Update Virus Database** area, specify how to update the Anti-Virus signatures. You can automatically check for signature updates from Cisco's signature server every 24 hours or manually check for signature updates at any time by clicking **Update**. See **Updating Anti-Virus Signatures, page 308**.

STEP 6 Click **Save** to apply your settings.

Configuring Advanced Anti-Virus Settings

Use the Advanced Settings page to configure the scan settings.

STEP 1 Click **Security Services > Anti-Virus > Advanced Settings**.

STEP 2 **Maximum File Size to Scan:** Enter the maximum file size, from 0 to 10240 kilobytes. Files larger than this size are passed without scanning. Use the default setting, 0, to indicate that there is no limit on the file size.

NOTE: For compressed files, Anti-Virus will scan each file after decompression and bypass virus scanning for the files larger than the maximum file size.

STEP 3 For each protocol, make the desired selections:

- **HTTP:**
  - Check the **Optimize Performance** box to suspend the Anti-Virus scan for websites with a good reputation. Uncheck the box to scan all sites. This option is available only when Web Reputation Filtering is enabled. For more information, see **Configuring Web Reputation Filtering, page 325**.
  - Check the **Disable HTTP Resume** box to disable resuming web-based file transfer by using the HTTP protocol when viruses are detected. Uncheck the box to allow resuming web-based file transfers in this situation.
- **FTP:** Check the **Disable FTP Resume** box to disable resuming file transfer by using the FTP protocol when viruses are detected. Uncheck the box to enable resuming file transfers in this situation.

STEP 4 Click **Save** to apply your settings.

Configuring HTTP Notification

HTTP Notification informs users that viruses are detected in web pages or in files that they try to access. Use the HTTP Notification page to customize the notification message that will be sent to the user when viruses are detected.

STEP 1 Click **Security Services > Anti-Virus > HTTP Notification**.

STEP 2 Enter the alert message in the **Notification Content** field.

- If you select Notify as the action for the HTTP protocol, the alert message is sent to the user.
- If you select Notify + Drop Connection as the action for the HTTP protocol, the connection is dropped and the alert message is sent to the user.

STEP 3 Click **Save** to apply your settings.

Configuring Email Notification

Email Notification allows you to send an alert email to the email receiver when viruses are detected in email attachments. Use the Email Notification page to customize the tag and notification message that are displayed in the alert email.

STEP 1 Click **Security Services > Anti-Virus > Email Notification**.

The Email Notification window opens. The following information is displayed:

- **Email Notification Status:** Shows if the Notify or Notify + Destruct File action is enabled or disabled for the SMTP or POP3 protocol.
  - If you choose Notify as the preventive action, the original email and an alert email are sent to the email receiver.
  - If you choose Notify + Destruct File as the preventive action, the infected files are deleted and the original email and an alert email are sent to the email receiver.
- **From Email Address:** The email address used to send the alert email.
- **SMTP Server:** The IP address or Internet name of the SMTP server.
- **SMTP Authentication:** Shows if the SMTP authentication is enabled or disabled.

NOTE: The above email server settings are read only. They are used to send the alert email to the original email receiver. You can click the **Edit** link to configure the email server settings, but save your settings on this page first. See Configuring Email Alert Settings, page 408.

STEP 2 If the Email Notification feature is enabled and the email server settings are configured, enter the following information:

- **Mail Tag:** Enter the tag that shows in the alert email's subject. The tag will insert to the alert email subject in the **[Tag] Email Subject** format.
- **Mail Content:** Enter the notification content that appears in the alert email.

STEP 3 Click **Save** to apply your settings.

Updating Anti-Virus Signatures

You can automatically check for Anti-Virus signature updates from Cisco's signature server every 24 hours or to manually check for Anti-Virus signature updates at any time by clicking **Update**. When a newer signature file is available on the server, the new signature file will be downloaded to your device.

NOTE A valid Cisco.com account is required to check for signature updates from Cisco's signature server. Go to the Device Management > Cisco Services & Support > Cisco.com Account page or click the **Edit Cisco.com Account Settings** link to configure your Cisco.com account credentials on the security appliance. See Configuring Cisco.com Account, page 424.

STEP 1 Click **Security Services > Anti-Virus > General Settings**.

STEP 2 In the **Update Virus Database** area, you can view the status of the Anti-Virus signature file. The following information is displayed:

- **Last Check:** The date and time of your last check.
- **Last Update:** The date and time of the last successful update.
- **Version:** The version number of the Anti-Virus signature file.
- **Virus Pattern Number:** The total amount of virus patterns in the Anti-Virus signature file.

STEP 3 To automatically update the Anti-Virus signatures, perform the following steps:

a. In the **Auto Update Virus Database** area, click **On** to automatically check for signature updates from Cisco's signature server every 24 hours.

b. Click **Save** to apply your settings.

STEP 4 To manually update the Anti-Virus signatures at any time, click **Update** to check for signature updates from Cisco's signature server immediately.

You can also click **Check for Updates Now** from the Security Services > Dashboard page to manually update the Anti-Virus signatures.

Configuring Application Control

Application Control monitors traffic through the Cisco ISA500 to permit or block traffic for individual applications and categories of applications. For some applications, you can permit or block certain features or functions of the application.

Important: Read the information in this guide to understand the features, required tasks, and recommendations before you implement this service.

To configure Application Control, refer to the following topics:

- **Configuring Application Control Policies, page 310**
- **General Application Control Settings, page 314**
- **Advanced Application Control Settings, page 318**

To configure reporting and email alerts, see these topics:

- **Viewing Application Control Report, page 301**
- **Configuring Email Alert Settings, page 408**

To ensure that Application Control can identify the latest applications, see **Updating Application Signature Database, page 317**.

Configuring Application Control Policies

Use the Application Control Policies page to configure the application control policies. An application control policy allows you to permit or block traffic for the applications by schedule.

Important Tips:

- Be aware that the Cisco ISA500 can control access only for the traffic that it handles. For example, if a PC and a server are directly connected to the LAN ports of the Cisco ISA500, Application Control policies apply to the traffic between these devices. However, if a switch is uplinked to the Cisco ISA500, the security appliance does not handle the traffic through the ports of that switch and therefore the Application Control policies do not apply.
- Application Control uses signatures to identify and block the applications. You must update the application signatures frequently so that Application Control can identify the latest applications. See **Updating Application Signature Database, page 317**.

Refer to the following topics:

- **General Application Control Policy Settings, page 310**
- **Adding an Application Control Policy, page 311**
- **Permitting or Blocking Traffic for all Applications in a Category, page 312**
- **Permitting or Blocking Traffic for an Application, page 313**

General Application Control Policy Settings

STEP 1 Click **Security Services > Application Control > Application Control Policies**.

STEP 2 You can perform the following actions:

- Click **Add Policy** to add a new application control policy. See **Adding an Application Control Policy, page 311**.
- Click the **Edit** (pencil) icon to edit an existing application control policy.
- Click the **Duplicate** icon to create a copy of an existing application control policy. This feature allows you to make a minor change for an existing application control policy to create a new policy.

- Click the **Delete** (x) icon to delete an existing application control policy. The default application control policy cannot be deleted.

STEP 3 Click **Save** to apply your settings.

Adding an Application Control Policy

An application control policy is used to permit or block traffic for the applications by schedule.

NOTE Up to 80 custom application control policies can be configured on the security appliance. Up to 8 application control policies can be applied to each zone.

STEP 1 Click **Add Policy** to create a new application control policy.

The Policy Profile - Add/Edit window opens.

STEP 2 Enter the following information:

- **Policy Name:** Enter the name for the application control policy.
- **Schedule:** Choose **Always on** to keep the application control policy always active or choose a schedule to permit or block the applications at a specific time of a day or at the specified days of a week. If the schedule that you want is not in the list, choose **Create a new schedule** to add a new schedule object. To maintain the schedules, go to the Device Management > Schedules page. See Configuring Schedules, page 449.

STEP 3 The security appliance supports a long list of applications. You can use the table filter settings to filter the applications and then specify the settings for the selected applications.

- **Category:** Allows you to filter the applications by category. Choose **All** to display all categories in the table or choose a category to only display the applications that belong to the selected category. You can click the triangle next to a category to expand or contract all applications in the category.
- **Application:** Allows you to filter the application by application name. Enter the name of the application in the field. Only the application that you specified is displayed in the table.
- **Current Action:** Allows you to filter the applications by action. Choose **Deny** to display all applications that are blocked or choose **Permit** to display all applications that are permitted.

NOTE: By default, the table filter settings are hidden. You can click the triangle next to **Hide Table Filter Settings** to display or hide the table filter settings.

STEP 4 After you set the table filter settings, click **Refresh Table** to refresh the data in the table. Only the applications that you specified are displayed in the table.

STEP 5 Specify the preventive action for a single application or for all applications in a category:

- To permit or block traffic for all applications in a category, click the **Edit** (pencil) icon in the **Configure** column for the category. For complete details, see **Permitting or Blocking Traffic for all Applications in a Category, page 312**.
- If the action, schedule, or logging settings vary among the applications in a category, you can configure the settings for each application in the category. You must first choose **keep application-level settings** for the Action and Logging options of the category, and then click the **Edit** (pencil) icon in the **Configure** column for the application. For complete details, see **Permitting or Blocking Traffic for an Application, page 313**.

STEP 6 Click **OK** to save your settings.

Permitting or Blocking Traffic for all Applications in a Category

This section describes how to configure the category default settings. The category default settings are applied to all applications in a category.

STEP 1 Click the **Edit** (pencil) icon in the **Configure** column for a category.

The Policy Profile - Add/Edit window opens.

STEP 2 Specify the category default settings:

- **Category:** The name of the category.
- **Action:** Choose **Permit** to permit traffic, or choose **Deny** to block traffic. If the action settings vary among the applications in the category, you must first choose the **keep application-level settings** option, and then configure the action for each application in the category. See **Permitting or Blocking Traffic for an Application, page 313**.

- **Logging:** Choose **Enable** to log the event when an application is blocked, or choose **Disable** to disable the logging feature. If the logging settings vary among the applications in a category, you must first choose the **keep application-level settings** option, and then configure the logging settings for each application in the category. See **Permitting or Blocking Traffic for an Application, page 313**.

  To log application blocking events, you must enable the logging settings for the applications, and then go to the Device Management > Logs pages to configure the log settings and the log facilities. See Log Management, page 442.

  - To save application blocking logs to the local syslog daemon, you must enable the Log feature, set the log buffer size and the severity for local logs, and enable the Local Log settings for the Application Control facility.
  - To save application blocking logs to the remote syslog server if you have a remote syslog server support, you must enable the Log feature, specify the Remote Log settings, and enable the Remote Log settings for the Application Control facility.

  NOTE: Changing the category default settings will override the application-level settings for all applications in the category.

STEP 3 Click **OK** to save your settings.

Permitting or Blocking Traffic for an Application

If the action, schedule, or logging settings vary among the applications in a category, you can configure the action and logging settings for each application in the category. The application-level settings are applied to a single application in a category.

NOTE To edit the settings for an application with detection disabled, you must first enable the detection from the Advanced Settings page.

NOTE Before you configure the application-level settings for each application in a category, make sure that you choose **keep application-level settings** for the Action and Logging options of the category.

STEP 1 Click the **Edit** (pencil) icon in the **Configure** column for an application.

The Policy Profile - Add/Edit window opens.

STEP 2 Specify the application-level control settings:

- **Application:** The name of the application.
- **Action:** Choose **Permit** to permit traffic for the application or choose **Deny** to block traffic for the application.
- **Logging:** Choose **Enable** to log the event when an application is blocked, or choose **Disable** to disable the logging function.

  To log application blocking events, you must first enable the logging settings for the applications, and then go to the Device Management > Logs pages to configure the log settings and the log facilities. See Log Management, page 442.
- **Configure feature-specific access control:** For some applications, you can permit or block certain features or functions of the application. For example, for Google Talk application, you can permit the chat function but block the media transfer function. Check this box and then specify the action for each feature or function of the application.

  NOTE: When the action for a specified feature or function is set to "Deny," it will no longer function.

STEP 3 Click **OK** to save your settings.

General Application Control Settings

Use the Application Control Settings page to enable the Application Control feature, apply the application control policies to different zones, and update the application signature database.

Important Tips:

- Be aware that the Cisco ISA500 can control access only for the traffic that it handles. For example, if a PC and a server are directly connected to the LAN ports of the Cisco ISA500, Application Control policies apply to the traffic between these devices. However, if a switch is uplinked to the Cisco ISA500, the security appliance does not handle the traffic through the ports of that switch and therefore the Application Control policies do not apply.
- You must update the application signatures frequently so that Application Control can identify the latest applications.

Refer to the following topics:

- Enabling Application Control Service, page 315
- Mapping Application Control Policies to Zones, page 315
- Configuring Application Control Policy Mapping Rules, page 316
- Updating Application Signature Database, page 317

Enabling Application Control Service

STEP 1 Click **Security Services > Application Control > Application Control Settings**.

STEP 2 Click **On** to enable the Application Control feature, or click **Off** to disable it. If you enable Application Control, by default all applications are allowed unless specifically blocked by an application control policy.

STEP 3 Click **Save** to apply your settings.

Mapping Application Control Policies to Zones

You can apply different application control policies to different zones. You can have multiple policies within a given zone for a different set of users. By default, the default application control policy that permits traffic for all applications is selected to all zones.

STEP 1 Click **Security Services > Application Control > Application Control Settings**.

STEP 2 In the **Zone Mapping** area, you can perform the following actions:

- Click the triangle next to a zone to expand or contract the application control policy mapping rules of the selected zone.
- Click **Add Mapping Rule** to add a new application control policy mapping rule. See **Configuring Application Control Policy Mapping Rules, page 316**.
- Click the **Edit** (pencil) icon to edit an existing application control policy mapping rule.
- Click the **Delete** (x) icon to delete an application control policy mapping rule. The default application control policy mapping rule for each zone cannot be deleted.

- Re-order the priorities of multiple application control policy mapping rules within a given zone. To move the rule up one position, click the **Move up** icon. To move the rule down one position, click the **Move down** icon. The default application control policy mapping rule must be the last policy with the lowest priority for a zone.

STEP 3 Click **Save** to apply your settings.

Configuring Application Control Policy Mapping Rules

An application control policy mapping rule applies a specific application control policy to a given zone to control application traffic from and to the zone. You can also apply a selected application control policy to a different set of users.

For example, you can control outgoing and incoming traffic to a given zone for a specific host or for the hosts within a specific IP range.

NOTE Make sure that you have configured the application control policies before you configure the policy mapping rules. See **Configuring Application Control Policies, page 310**.

STEP 1 Click **Add Mapping Rule** to add a new application control policy mapping rule.

The Application Control Policy Mapping - Add/Edit window opens.

STEP 2 Enter the following information:

- **Zone:** Choose an existing zone to control application traffic from and to the selected zone. This mapping rule will be listed under the selected zone.
- **Policy:** Choose an existing application control policy to apply the selected policy to the zone.
- **Matching Condition:** You can apply the selected application control policy to all users, a specific host, or the hosts within a specific IP range. Choose one of the following options:
  - **All IP Addresses and Users:** Applies the selected application control policy to all users.
  - **Specific IP Address Object:** Applies the selected application control policy to a specific host or to the hosts within a specific IP range. Traffic for the specific host or for the hosts within the IP range will be detected. Traffic for other users will be bypassed. The IP address object can be a host or a range of IP addresses. If the address object that you want is not

in the list, choose **Create a new address** to create a new address object. To maintain the address objects, go to Networking > Address Management page. See **Address Management, page 175**.

STEP 3 Click **OK** to save your settings.

Updating Application Signature Database

Application Control uses signatures to identify and block the applications. You must update the application signatures frequently so that Application Control can identify the latest applications. You can automatically check for signature updates from Cisco's signature server on a weekly basis or manually check for signature updates at any time by clicking **Check for Update Now**. If a newer signature file is available on the server, the new signature file will be automatically downloaded to your device.

You can also first download the latest signature file from Cisco's signature server to your local PC, and then manually update the application signatures through the Configuration Utility.

A valid Cisco.com account is required to check for signature updates from Cisco's signature server. Go to the Device Management > Cisco Services & Support > Cisco.com Account page to configure your Cisco.com account credentials on the security appliance. See Configuring Cisco.com Account, page 424.

NOTE Application Control and IPS use the same signature database. Updating the application signatures will also update the IPS signatures at the same time.

STEP 1 Click **Security Services > Application Control > Application Control Settings**.

STEP 2 In the **Update Signature Database** area, the following information is displayed:

- **Last Check:** The date and time of the last check.
- **Last Update:** The date and time of the last successful update when the signature file is updated successfully.
- **Version:** The version number of the application signature file that is currently used on the security appliance.

STEP 3 To automatically update the application signatures, perform the following steps:

a. In the **Auto Update** area, click **On** to automatically check for signature updates from Cisco's signature server every Monday at 00:00.

b. Click **Save** to apply your settings.

STEP 4 To manually update the application signatures at any time, click **Check for Update Now** to check for signature updates from Cisco's signature server immediately.

You can also click **Check for Updates Now** from the Security Services > Dashboard page to manually update the application signatures.

STEP 5 To manually update the application signatures from your local PC, perform the following steps:

a. You must first download the application signature file from Cisco's signature server to your local PC.

b. In the **Manually Update Signature Database** area, click **Browse** to locate and select the signature file from your local PC.

c. Click **Update Database**.

Advanced Application Control Settings

Use the Application Control Advanced Settings page to enable or disable the detection for each application.

STEP 1 Click **Security Services > Application Control > Application Control Advanced Settings**.

The Application Control Advanced Settings window opens.

STEP 2 The security appliance supports a long list of applications. You can use the table filter settings to filter the applications in the table and then specify the detection settings for all selected applications:

- **Category:** Allows you to filter the applications by category. Choose the category that you want from the drop-down list. Only the applications that belong to the selected category are displayed. You can click the triangle next to a category to expand or contract all applications under the category.
- **Application:** Allows you to filter the application by application name. Enter the name of the application in the field. Only the application that you specified is displayed in the table.
- **Detection:** Allows you to filter the applications by detection status. Choose **Enable** to display all applications with detection enabled or choose **Disable** to display all applications with detection disabled.

NOTE: By default, the table filter settings are hidden. You can click the triangle next to **Show Table Filter Settings** to display or hide the table filter settings.

STEP 3 After you set the table filter settings, click **Refresh Table** to refresh the data in the table.

STEP 4 You can enable or disable the detection for the selected applications in the table. In the **Detection** column, choose **Enable** to enable the detection for an application or choose **Disable** to disable the detection for an application.

STEP 5 Click **Save** to apply your settings.

Configuring Spam Filter

Spam Filter detects the email sender's reputation score. The reputation scores range from -10 (bad) to +10 (good). An email is classified as spam if the sender's reputation is below the spam threshold, or is classified as suspected spam if the sender's reputation is between the spam threshold and suspected spam threshold. An email is not classified as spam if the sender's reputation is above the suspected spam threshold.

Spam Filter detects spam emails based on the reputation score of the sender's IP address. The sender's address is the address of the host that connects to the SMTP server to deliver an email message, not an address within the email header.

STEP 1 Click **Security Services > Spam Filter**.

STEP 2 Click **On** to enable Spam Filter, or check **Off** to disable it.

STEP 3 If you enable Spam Filter, enter the following information:

- **SMTP Server Address/Domain:** Enter the IP address or domain name of your internal SMTP server. The SMTP server must have its Internet traffic routed through the security appliance. The SMTP server or the clients that use this SMTP server can be configured to respond to the spam and suspected spam tags that the security appliance applies to the email.
- **Action when Spam Detected:** Choose **Block Email** to block the email, or choose **Tag Email with [Spam]** to get the email tagged with [Spam].

- **Action when Suspect Spam Detected:** Choose **Block Email** to block the email, or choose **Tag Email with [Suspect Spam]** to get the email tagged with [Suspect Spam].
- **Reputation Threshold:** Specify the block sensitivity as Low, Medium, or High, or as a numerical threshold (Custom).
  - **Low:** Blocks less spam with lowest risk of false positives. The threshold value for spam is -4 and the threshold value for suspected spam is -2.
  - **Medium:** Blocks more spam with moderate risk of false positives. The threshold value for spam is -3 and the threshold value for suspected spam is -1.
  - **High:** Blocks most spam with increased risk of false positives. The threshold value for spam is -2 and the threshold value for suspected spam is -0.5.
  - **Custom:** Manually set the spam reputation threshold. When the Custom radio button is selected, choose the threshold values for spam and suspected spam. The allowable values for the threshold are integers from -10 to -1 and the value -0.5.

STEP 4 In the **Allowed Senders** area, you can specify the email sender exceptions against your Spam Filter settings. Traffic from the specified hostnames or IP addresses will not be examined by Spam Filter.

- To add an exception, enter the hostname or IP address of the sender in the **Hostname/IP Address** field and click **Add**.
- To remove an exception, select it from the list of **Allowed Senders** and click **Remove**.

STEP 5 In the **Service Outage** area, choose one of the following actions when Spam Filter is unavailable:

- **Do Not Accept Emails when spam reputation services are not available:** All emails are delayed until Spam Filter is available.
- **Accept Emails even when spam reputation services are not available:** All emails are delivered without checking for spam.

STEP 6 Click **Save** to apply your settings.

Configuring Intrusion Prevention

Intrusion Prevention System (IPS) is a network-based platform that inspects network traffic for malicious or unwanted activity such as worms, spyware, and policy violations. When IPS detects a threat, it reacts in real-time by taking actions such as blocking or dropping connections, logging the detected activities, and sending notifications about these activities. You can use the default actions for each signature or customize the actions to suit your requirements.

IMPORTANT: IPS uses signatures to identify the attacks in progress. You must update the IPS signatures frequently to keep the protection current. See **Updating IPS Signature Database, page 324**.

After setting up IPS, you have these options for monitoring the activity:

- Enable the IPS report from the Security Services > Security Services Reports page or from the Status > Security Services Reports page to see the number of packets detected and the number of packets dropped by IPS. See **Viewing IPS Report, page 300**.
- Enable the IPS Alert feature to send an alert email to a specified email address if an attack is detected by IPS. See Configuring Email Alert Settings, page 408.

NOTE You must install licenses on the License Management page before you can configure IPS.

STEP 1 Click **Security Services > Intrusion Prevention (IPS) > IPS Policy and Protocol Inspection**.

The IPS Policy and Protocol Inspection window opens.

STEP 2 At the top of the page, enable or disable IPS by clicking **On** or **Off**.

STEP 3 In the **Zone** area, chose the zones to be inspected. IPS inspects inter-zone traffic only.

- **To add a zone:** In the Zones Available list, click a zone, and then click **Add** to move it to the Selected Zones list. All incoming and outgoing traffic for the selected zones is inspected.
- **To remove a zone:** In the Selected Zones list, click a zone, and then click **Remove** to move it to the Zones Available list.

NOTE: You can block an intrusion based on the source zones or based on the destination zones. For example, if you select the LAN and DMZ zones, IPS inspects all traffic for the LAN and DMZ zones regardless of its source. Traffic between LAN and DMZ is inspected once, not twice. If you select the WAN zone, IPS inspects all traffic for the WAN zone regardless of its destination.

STEP 4 In the **IPS Signature** area, use the options below to filter the list of signatures in the Selected Signature table. The unfiltered list includes thousands of IPS signatures that are used to identify attacks. After selecting filters, click **Refresh** to redisplay the Selected Signature table showing only the matching signatures.

- **Severity Level:** Choose a severity level, from highest to lowest: Critical, High, Medium, Low, and Information.
- **Operating System Type:** Choose **All** to include all signatures regardless of the type of operating system, or choose **Selected OS Types Only** to include only the signatures that match the specified types of operation systems.
- **Host Type:** Choose a host type.
- **Category:** Choose **All** to include all signatures regardless of the category, or choose **Selected Categories Only** to include only the signatures that match the specified categories.

The Selected Signature table displays this information:

- **Name:** The name of the signature.
- **ID:** The unique identifier of the signature. To view complete details for a signature, click the link in the ID column.
- **Severity:** The severity level of the threat that the signature can identify.
- **Category:** The category that the signature belongs to.
- **Default Action:** The default preventive action for the signature.
  - **Block and Log:** Deny the request, drop the connection, and log the event when a signature is detected by the IPS engine.
  - **Log Only:** Only log the event when a signature is detected by the IPS engine.
- **Current Action:** The current preventive action for the signature.
- **Edit Action:** Click the pencil icon to enable, disable, or set the preventive actions for a signature. For more information, see **Configuring Signature Actions, page 323**.

NOTE: For ease of use, you can edit the preventive actions for a group of signatures. Check the box for each signature that you want to change, or select all signatures by checking the box in the top left corner of the table. To edit the settings for the selected signatures, click the **Edit** (pencil) icon at the top of the table.

- **Block Threshold:** Specify a threshold at which blocking occurs; whether the Current Action is to block and log or to log only, traffic is blocked after the specified number of occurrences. Enter 0 to apply the Current Action immediately upon detection.

  NOTE: The counter is reset to 0 whenever IPS settings are saved in the configuration utility or the security appliance is rebooted.

STEP 5 Click **Save** to apply your settings.

Configuring Signature Actions

After selecting one or more signatures on the Security Services > Intrusion Prevention (IPS) > IPS Policy and Protocol Inspection page, use the Edit Selected Signature Actions page to enable or disable the selected signatures and to configure the actions.

STEP 1 Enter the following information:

- **Enable detection of selected signatures:** Check this box to enable the intrusion detection for this signature, or uncheck this box to disable it.
- **Name:** The name of the signature.
- **ID:** The unique identifier of the signature.
- **Severity:** The severity level of the threat that the signature can identify.
- **Default Action:** The default preventive action for the signature.
- **Action on Detect:** Choose one of the following actions for the signature:
  - **Block and Log:** Deny the request, drop the connection, and log the event when the security signature is detected by the IPS engine.
  - **Log only:** Only log the event when the security signature is detected by the IPS engine. This option is mostly used for troubleshooting purposes.

To log IPS events, you must first specify the action for the signatures, and then go to the Device Management > Logs pages to configure the log settings and log facilities. See Log Management, page 442.

To save IPS logs to the local syslog daemon, you must enable the Log feature, set the log buffer size and the severity for local logs, and then enable the Local Log settings for the Intrusion Prevention (IPS) facility.

To save IPS logs to a remote syslog server, you must enable the Log feature, specify the Remote Log settings, and enable the Remote Log settings for the Intrusion Prevention (IPS) facility.

STEP 2 Click **OK** to save your settings.

STEP 3 Click **Save** to apply your settings.

Updating IPS Signature Database

You can automatically check for signature updates from Cisco's signature server on a weekly basis or manually check for signature updates at any time by clicking **Check for Update Now**. If a newer signature file is available, the new signature file will be automatically downloaded to your device.

You can also first download the latest signature file from Cisco's signature server to your local PC, and then manually update the IPS signatures through the Configuration Utility.

A valid Cisco.com account is required to check for signature updates and download the IPS signature file from Cisco's signature server. Go to the Device Management > Cisco Services & Support > Cisco.com Account page to configure your Cisco.com account credentials on the security appliance. See **Configuring Cisco.com Account, page 424**.

NOTE IPS and Application Control use the same signature database. Updating the IPS signatures will also update the application signatures at the same time.

STEP 1 Click **Security Services > Intrusion Prevention (IPS) > IPS Policy and Protocol Inspection**.

The IPS Policy and Protocol Inspection window opens.

STEP 2 In the **Automatic Update Signature Database** area, the following information is displayed:

- **Last Check:** The date and time of the last check.
- **Last Update:** The date and time of the last successful update when the signature file is updated successfully.
- **Version:** The version number of the IPS signature file that is currently used on the security appliance.

STEP 3 To automatically update the IPS signatures, perform the following steps:

a. In the **Auto Update** area, click **On** to automatically check for signature updates from Cisco's signature server every Monday at 00:00.

b. Click **Save** to apply your settings.

STEP 4 To manually update the IPS signatures at any time, click **Check for Update Now** to check for signature updates from Cisco's signature server immediately.

You can also click **Check for Updates Now** from the Security Services > Dashboard page to manually update the IPS signatures.

STEP 5 To manually update the IPS signatures from your local PC, perform the following steps:

a. You must first download the signature file from Cisco's signature server to your local PC.

b. In the **Manually Update Signature Database** area, click **Browse** to locate and select the signature file from your local PC.

c. Click **Update Database**.

Configuring Web Reputation Filtering

Web Reputation Filtering prevents client devices from accessing dangerous websites containing viruses, spyware, malware, or phishing links. Web Reputation Filtering detects the web threats based on the reputation score of a web page. Reputation scores range from -10 (bad) to +10 (good). Web pages with reputation scores below a specific threshold are considered threats and blocked.

Web Reputation Filtering only monitors and controls the website visits through the specified HTTP port. Go to the Security Services > Web URL Filtering > Advanced Settings page to view or specify the HTTP port. See **Configuring Advanced Web URL Filtering Settings, page 330**.

You can create a “white list” of trusted sites by adding up to 256 Allowed Web Sites. The specified websites will not be examined by Web Reputation Filtering.

STEP 1 Click **Security Services > Web Reputation Filtering**.

STEP 2 Click **On** to enable Web Reputation Filtering, or click **Off** to disable it.

STEP 3 Specify the block sensitivity as Low, Medium, or High, or as a numerical threshold (Custom). The threshold values for Low, Medium, or High are predefined and cannot be edited.

- **Low:** Blocks fewer web threats. The threshold value is -6.
- **Medium:** Blocks more web threats. The threshold value is 5.
- **High:** Blocks most web threats. The threshold value is -4.
- **Custom:** Manually set the web reputation threshold. After selecting this option, choose a threshold value from -10 to -0.5.

Note: The rate of false positives increases as the threshold approaches 0.

STEP 4 In the **Allowed Web Sites** area, you can specify the website exceptions against your Web Reputation Filtering settings. The specified websites will not be examined by Web Reputation Filtering. You can include up to 16 websites on this list.

- To add a website exception, enter the following information:
  - **Matching Domain:** Allows you to permit the HTTP access of a website that fully matches a specific domain name. If you choose this option, enter the domain name, not including http://, in the **Site URL** field and then click **Add**.
  - **Containing Keyword:** Allows you to permit the HTTP access of a website that contains a specific keyword. If you choose this option, enter the URL keyword, not including http://, in the **Site URL** field and then click **Add**.
- To remove a website exception, select it from the list of **Allowed Sites** and click **Remove**.

STEP 5 In the **Service Outage** area, you can specify how to deal with web traffic when Web Reputation Filtering is unavailable. Choose one of the following actions:

- **Block Web Traffic when web reputation filter services are not available:** All web traffic is blocked until Web Reputation Filtering is available. The default block page will be displayed when a web page is blocked. The message that you specify in the **Blocked Web Filter Message** field will show on the default block page.
- **Allow Web Traffic even when web reputation filter services are not available:** All web traffic is allowed until Web Reputation Filtering is available.

STEP 6 Click **Save** to apply your settings.

Configuring Web URL Filtering

Web URL Filtering allows you to block HTTP access to malicious websites based on URL categories. You can allow or block an entire URL category to make configuration simpler. You can also specify the website exceptions against the URL category settings. For example, you can block the websites that Web URL Filtering usually allows, or allow the websites that Web URL Filtering usually blocks.

You can enable Web URL Filtering Alert to send email alerts to a specific email address when web URL categories have any changes. See Configuring Email Alert Settings, page 408.

Web URL Filtering only monitors and controls the website visits through the HTTP port specified on the Web URL Filtering > Advanced Settings page.

Refer to the following topics:

- **Configuring Web URL Filtering Policy Profiles, page 328**
- **Configuring Website Access Control List, page 329**
- **Mapping Web URL Filtering Policy Profiles to Zones, page 330**
- **Configuring Advanced Web URL Filtering Settings, page 330**

Configuring Web URL Filtering Policy Profiles

A Web URL Filtering policy profile is used to specify which URL categories are blocked or allowed.

NOTE Up to 256 Web URL Filtering policy profiles can be configured on the security appliance.

STEP 1 Click **Security Services > Web URL Filtering > Policy Profile**.

STEP 2 To add a new Web URL Filtering policy profile, click **Add**.

Other Options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. The default profile cannot be deleted.

The Policy Profile - Add/Edit window opens.

STEP 3 Enter the following information:

- **Policy Name:** Enter the name for the policy profile.
- **Description:** Enter a brief description for the policy profile.
- **Select URL Categories to Block:** Check an URL category to block it, or uncheck this box to permit it. If an URL category is blocked (or permitted), all websites that belong to this category are blocked (or permitted).

STEP 4 Specify the website exceptions if needed. The website exceptions allow you to permit or block specific websites against the URL category settings. All website exceptions can be added to the website access control list. The website access control list has higher priority than the URL category settings. See **Configuring Website Access Control List, page 329**.

For example, if the Sports and Recreation category is blocked, but you want to permit the website: www.espn.com, you can add it to the website access control list as an exception.

STEP 5 Click **Save** to apply your settings.

Configuring Website Access Control List

Blocking an URL category will block all websites that belong to this category. You can specify the website exceptions in the website access control list. The website exceptions will override the URL category settings in the same profile.

NOTE Up to 32 website exceptions can be configured for each Web URL Filtering policy profile.

STEP 1 In the **Specify URLs or URL keywords you want to permit or deny** area, click **Edit**.

The Policy Profile - Add/Edit window opens.

STEP 2 To add a website access rule, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete all entries, click **Delete All**.

The Website Access Control Rule - Add/Edit window opens.

STEP 3 Enter the following information:

- **Enable Content Filter URL:** Click **On** to enable the website access rule, or click **Off** to create only the website access rule.
- **URL:** Enter the domain name or URL keyword of a website that you want to permit or block.
- **Match Type:** Specify the method for applying this rule:
  - **Domain:** Permit or deny the HTTP access of a website that fully matches the domain name that you entered in the **URL** field.

    For example, if you enter yahoo.com in the URL field, then it can match the website http://yahoo.com/*, but cannot match the website http://*.yahoo.com.uk/*.
  - **URL Keyword:** Permit or deny the HTTP access of a website that contains the keyword that you entered in the **URL** field.

    For example, if you enter yahoo in the URL field, then it can match the websites such as www.yahoo.com, tw.yahoo.com, www.yahoo.com.uk, and www.yahoo.co.jp.
- **Action:** Choose **Permit** to permit access, or choose **Block** to block access.

STEP 4 Click **OK** to save your settings.

Mapping Web URL Filtering Policy Profiles to Zones

Use the Policy to Zone Mapping page to apply the Web URL Filtering policy profile to each zone. The Web URL Filtering policy assigned to each zone determines whether to block or forward the HTTP requests from the hosts in the zone. By default, Default Profile that permits all URL categories is assigned to all predefined zones and new zones.

STEP 1 Click **Security Services > Web URL Filtering > Policy to Zone Mapping**.

The Policy to Zone Mapping window opens.

STEP 2 Click **On** to enable Web URL Filtering, or click **Off** to disable it.

NOTE: Enabling Web URL Filtering will disable Firewall Content Filtering and vice-versa.

STEP 3 In the **Zone Policy Map** area, choose a Web URL Filtering policy for each zone.

STEP 4 Click **Save** to apply your settings.

Configuring Advanced Web URL Filtering Settings

STEP 1 Click **Security Services > Web URL Filtering > Advanced Settings**.

STEP 2 Enter the following information:

- **Filter Traffic on HTTP port:** Enter the port number that is used for filtering HTTP traffic. Web URL Filtering only monitors and controls the website visits through this HTTP port. The default value is 80.
- **Filter Traffic on HTTPS port:** Enter the port number that is used for filtering HTTPS traffic. Web URL Filtering only monitors and controls the website visits through this HTTPS port. The default value is 443.
- **Blocked Web Components:** You can block or permit the web components like Proxy, Java, ActiveX, and Cookies. By default, all of them are permitted.

- **Proxy:** Check this box to block proxy servers, which can be used to circumvent certain firewall rules and thus present a potential security gap.
- **Java:** Check this box to block Java applets that can be downloaded from pages that contain them.
- **ActiveX:** Check this box to prevent ActiveX applets from being downloaded through Internet Explorer.
- **Cookies:** Check this box to block cookies, which typically contain sessions.

STEP 3 Choose one of the following actions when Web URL Filtering is unavailable:

- **Block Web Traffic when web URL filter services are not available:** All web traffic is blocked until Web URL Filtering is available.
- **Allow Web Traffic even when web URL filter services are not available:** All web traffic is allowed until Web URL Filtering is available.

STEP 4 Choose one of the following actions when a web page is blocked:

- **Display Blocked URL Message when the requested page is blocked:** Displays the default block page when a web page is blocked. If you choose this option, the message that you specify in the **Blocked URL Message** field will show on the default block page.
- **Redirect URL:** Redirects to a specified web page when a web page is blocked. If you choose this option, enter a desired URL to be redirected. Make sure that the specified URL is allowed by the Website Access Control List.

STEP 5 Click **Save** to apply your settings.

Network Reputation

Network Reputation blocks incoming traffic from IP addresses that are known to initiate attacks throughout the Internet. Network Reputation checks the source and destination addresses of each packet against the address blacklist to determine whether to proceed or to drop the packet. The blacklist data is automatically updated every six hours. You can click **Check for Updates Now** on the Security Services > Dashboard page to immediately check for new updates for Network Reputation.

NOTE No configuration is needed for Network Reputation. You only need to enable or disable this feature from the Security Services > Dashboard page.

8

VPN

This chapter describes how to configure Virtual Private Networks (VPNs) that allow other sites and remote workers to access your network resources. It includes the following sections:

- About VPNs, page 334
- Viewing VPN Status, page 335
- Configuring a Site-to-Site VPN, page 340
- Configuring IPsec Remote Access, page 355
- Configuring Teleworker VPN Client, page 363
- Configuring SSL VPN, page 372
- Configuring L2TP Server, page 385
- Configuring VPN Passthrough, page 387

To access the VPN pages, click **VPN** in the left hand navigation pane.

About VPNs

A VPN provides a secure communication channel (also known as a “tunnel”) between two gateway routers or between a remote PC and a gateway router. The security appliance supports the following VPN solutions:

- **Site-to-Site VPN:** Connects two routers to secure traffic between two sites that are physically separated. See **Configuring a Site-to-Site VPN, page 340**.
- **IPsec Remote Access:** Allows the security appliance to act as a head-end device in remote access VPNs. Your security appliance will be set as an IPsec VPN server and push the security policies to remote VPN clients, so that remote VPN clients have up-to-date policies in place before establishing the VPN connections. The IPsec VPN server can also terminate the VPN connections initiated by remote VPN clients. This flexibility allows mobile and remote users to access critical data and applications on corporate Intranet. See **Configuring IPsec Remote Access, page 355**.
- **Teleworker VPN Client:** Minimizes the configuration requirements at remote locations by allowing the security appliance to work as a Cisco VPN hardware client to receive the security policies over the VPN tunnel from a remote IPsec VPN server. See **Configuring Teleworker VPN Client, page 363**.
- **SSL VPN:** Allows remote users to access the corporate network by using the Cisco AnyConnect Secure Mobility Client software. Remote access is provided through a SSL VPN gateway. See **Configuring SSL VPN, page 372**.
- **L2TP:** Allows remote clients to use a public IP network to secure communicate with private corporate network servers. See **Configuring L2TP Server, page 385**.

NOTE The security appliance can function as an IPsec VPN server or as a Cisco VPN hardware client, but not both simultaneously.

Viewing VPN Status

This section describes how to view information for all VPN sessions. Refer to the following topics:

- **Viewing IPsec VPN Status, page 335**
- **Viewing SSL VPN Status, page 337**

Viewing IPsec VPN Status

Use the IPsec VPN Status page to view the status of all IPsec VPN sessions. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

VPN > VPN Status > IPsec VPN Status

Field	Description
Active Sessions To manually terminate an active IPsec VPN session, click the **Disconnect** icon in the **Connect** column. To manually terminate multiple active IPsec VPN sessions, check them and click the **Disconnect** button. If an IPsec VPN session is terminated, you can manually establish the VPN connection by clicking the **Connect** icon in the **Connect** column.	
Name	VPN policy used for an IPsec VPN session.
Status	Connection status for an IPsec VPN session.
VPN Type	VPN connection type for an IPsec VPN session, such as Site-to-Site, IPsec Remote Access, or Teleworker VPN Client.
WAN Interface	WAN port used for an IPsec VPN session.

Field	Description
Remote Gateway	IP address of the remote peer. **NOTE:** For a site-to-site VPN session, it displays the IP address of the remote gateway. For an IPsec VPN session between the Teleworker VPN client and a remote IPsec VPN server, it displays the IP address of the IPsec VPN server. For an IPsec VPN session between the IPsec VPN server and a remote VPN client, it displays the IP address of the remote VPN client.
Local Network	Subnet IP address and netmask of your local network.
Remote Network	Subnet IP address and netmask of the remote network.
Statistics	
Name	VPN policy used for an IPsec VPN session.
VPN Type	VPN connection type for an IPsec VPN session.
WAN Interface	WAN port used for an IPsec VPN session.
Remote Gateway	IP address of the remote peer.
Local Network	Subnet IP address and netmask of your local network.
Remote Network	Subnet IP address and netmask of the remote network.
Tx Bytes	Volume of traffic in kilobytes transmitted from the VPN tunnel.
Rx Bytes	Volume of traffic in kilobytes received from the VPN tunnel.
Tx Packets	Number of IP packets transmitted from the VPN tunnel.
Rx Packets	Number of IP packets received from the VPN tunnel.

Field	Description
Teleworker VPN Client If the Teleworker VPN Client feature is enabled and the security appliance is acting as a Cisco VPN hardware client, the following information is displayed.	
Status	Shows if the Teleworker VPN Client feature is enabled or disabled.
Primary DNS	IP address of the primary DNS server.
Secondary DNS	IP address of the secondary DNS server.
Primary WINS	IP address of the primary WINS server.
Secondary WINS	IP address of the secondary WINS server.
Default Domain	Default domain name.
Split Tunnel	IP address and netmask for the specified split subnets.
Split DNS	Domain name for the specified split DNS.
Backup Server 1/2/3	IP address or hostname for the specified backup servers.

Viewing SSL VPN Status

Use the SSL VPN Status page to view information for all active SSL VPN sessions. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

VPN > VPN Status > SSL VPN Status

Field	Description
Active Sessions To manually terminate an active SSL VPN session, click the **Disconnect** icon in the **Configure** column. To manually terminate multiple active SSL VPN sessions, check them and click the **Disconnect** button.	
Session ID	ID of the SSL VPN session.
User Name	Name of the connected SSL VPN user.

Field	Description
Client IP (Actual)	Actual IP address used by the SSL VPN client.
Client IP (VPN)	Virtual IP address of the SSL VPN client assigned by the SSL VPN gateway.
Connect Time	Amount of time since the SSL VPN user first established the connection.

SSL VPN Statistics

In the **Global Status** area, the global statistic information is displayed. To clear the global statistic information, click **Clear**.

Active Users	Total number of connected SSL VPN users.
In CSTP Frames	Number of CSTP frames received from all clients.
In CSTP Bytes	Total number of bytes in the CSTP frames received from all clients.
In CSTP Data	Number of CSTP data frames received from all clients.
In CSTP Control	Number of CSTP control frames received from all clients.
Out CSTP Frames	Number of CSTP frames sent to all clients.
Out CSTP Bytes	Total number of bytes in the CSTP frames sent to all clients.
Out CSTP Data	Number of CSTP data frames sent to all clients.
Out CSTP Control	Number of CSTP control frames sent to all clients.

In the **Session Statistics** table, the following information for each SSL VPN session is displayed.

To clear the statistic information for a single SSL VPN session, click **Clear** in the **Configure** column. To clear the statistic information for multiple SSL VPN sessions, check them and click **-Clear**.

Session ID	ID of the SSL VPN session.
In CSTP Frames	Number of CSTP frames received from the client.

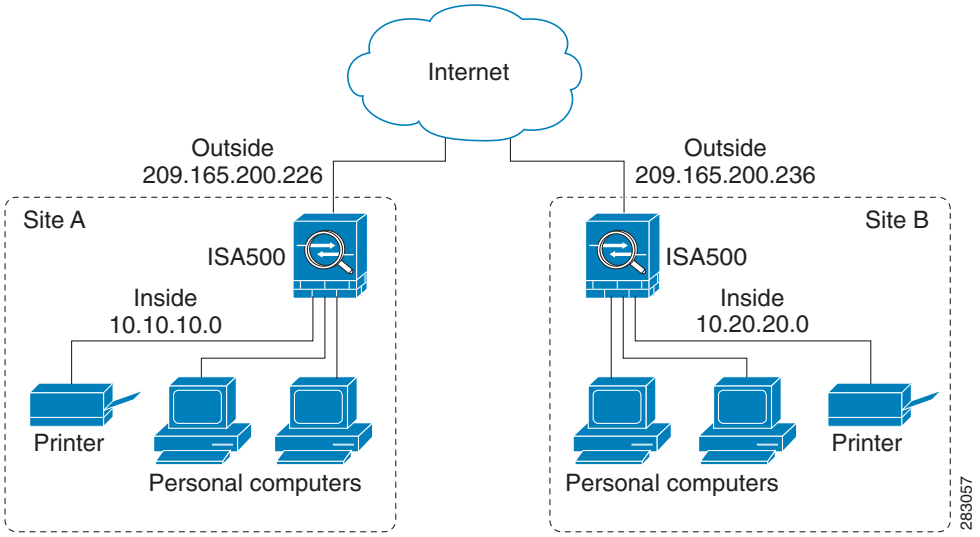
Field	Description
In CSTP Bytes	Total number of bytes in the CSTP frames received from the client.
In CSTP Data	Number of CSTP data frames received from the client.
In CSTP Control	Number of CSTP control frames received from the client.
Out CSTP Frames	Number of CSTP frames sent to the client.
Out CSTP Bytes	Total number of bytes in the CSTP frames sent to the client.
Out CSTP Data	Number of CSTP data frames sent to the client.
Out CSTP Control	Number of CSTP control frames sent to the client.

NOTE CSTP is a Cisco proprietary protocol for SSL VPN tunneling. “In” represents that the packet comes from the client. “Out” represents that the packet is sent to the client. The client is the PC running the Cisco AnyConnect Secure Mobility Client software that connects to the security appliance running the SSL VPN server. A CSTP frame is a packet carrying the CSTP protocol information. There are two major frame types, control frames and data frames. Control frames implement control functions within the protocol. Data frames carry the client data, such as the tunneled payload.

Configuring a Site-to-Site VPN

A site-to-site VPN tunnel connects two routers to secure traffic between two sites that are physically separated.

Figure 3 Site-to-Site VPN



This section describes how to set up the site-to-site VPN tunnels. Refer to the following topics:

- **Configuration Tasks to Establish a Site-to-Site VPN Tunnel, page 341**
- **General Site-to-Site VPN Settings, page 341**
- **Configuring IPsec VPN Policies, page 343**
- **Configuring IKE Policies, page 349**
- **Configuring Transform Sets, page 351**
- **Remote Teleworker Configuration Examples, page 352**

Configuration Tasks to Establish a Site-to-Site VPN Tunnel

To establish a site-to-site VPN tunnel, complete the following configuration tasks:

- Add the subnet IP address objects for your local network and remote network. See **Address Management, page 175**.
- (Optional) Import the certificates for authentication between two peers. Skip this step if you want to use the pre-shared key for authentication. See **Managing Certificates for Authentication, page 418**.
- Enable the site-to-site VPN feature on the security appliance. See **General Site-to-Site VPN Settings, page 341**.
- Configure IKE policies. See **Configuring IKE Policies, page 349**.
- Configure transform policies. See **Configuring Transform Sets, page 351**.
- Configure IPsec VPN policies. See **Configuring IPsec VPN Policies, page 343**.
- (Optional) Check an enabled IPsec VPN policy and click the **Connect** icon to initiate the VPN connection.

  When a site-to-site IPsec VPN policy is in place and enabled, a connection will be triggered by any traffic that matches the policy. In this case, the VPN tunnel will be set up automatically. However, for an IPsec VPN policy in which this router's Remote Network is set to Any (a "site-to-any" tunnel), a connection cannot be set up automatically. Instead you must manually establish the VPN connection by clicking the **Connect** icon.
- View the status and statistic information for all IPsec VPN sessions. See **Viewing IPsec VPN Status, page 335**.

General Site-to-Site VPN Settings

STEP 1 Click **VPN > Site-to-Site > IPsec Policies**.

The IPsec Policies window opens. All existing IPsec VPN policies are listed in the table. The following information is displayed:

- **Name:** The name of the IPsec VPN policy.
- **Enable:** Shows if the IPsec VPN policy is enabled or disabled.
- **Status:** Shows if the IPsec VPN tunnel is connected or disconnected.

- **WAN Interface:** The WAN port that traffic passes through over the IPsec VPN tunnel.
- **Peers:** The IP address of the remote peer.
- **Local:** The local network of the local peer.
- **Remote:** The remote network of the remote peer.
- **IKE:** The IKE policy used for the IPsec VPN policy.
- **Transform:** The transform set used for the IPsec VPN policy.

STEP 2 Click **On** to enable site-to-site VPN, or click **Off** to disable it.

NOTE: Enabling the Site-to-Site VPN feature will disable the Teleworker VPN Client feature.

STEP 3 If you enable site-to-site VPN, perform the following actions:

- To add a new IPsec VPN policy, click **Add**. See **Configuring IPsec VPN Policies, page 343**.
- To edit an existing IPsec VPN policy, click the **Edit** (x) icon.
- To delete an IPsec VPN policy, click the **Delete** (x) icon.
- To delete multiple IPsec VPN policies, check them and click **Delete**.
- To enable an IPsec VPN policy, check the box in the **Enable** column.
- To manually establish a VPN tunnel, click the **Connect** icon for an enabled IPsec VPN policy.
- To manually terminate a VPN connection, click the **Disconnect** icon.
- To refresh the data for site-to-site VPN, click **Refresh**.

STEP 4 Click **Save** to apply your settings.

Configuring IPsec VPN Policies

The IPsec VPN policy is used to establish the VPN connection between two peers. ISA550 and ISA550W support up to 50 IPsec VPN tunnels. ISA570 and ISA570W support up to 100 IPsec VPN tunnels.

NOTE Before you create an IPsec VPN policy, make sure that the IKE and transform policies are configured. Then you can apply the IKE and transform policies to the IPsec VPN policy.

STEP 1 **Click VPN > Site-to-Site > IPsec Policies.**

STEP 2 To add a new IPsec VPN policy, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The IPsec Policies - Add/Edit window opens.

STEP 3 In the **Basic Settings** tab, enter the following information:

- **Description:** Enter the name for the IPsec VPN policy.
- **IPsec Policy Enable:** Click **On** to enable the IPsec VPN policy, or click **Off** to create only the IPsec VPN policy.
- **Remote Type:** Specify the remote peer:
  - **Static IP:** Choose this option if the remote peer uses a static IP address. Enter the IP address of the remote peer in the **Remote Address** field.
  - **Dynamic IP:** Choose this option if the remote peer uses a dynamic IP address.
  - **FQDN (Fully Qualified Domain Name):** Choose this option to use the domain name of the remote network, such as vpn.company.com. Enter the domain name of the remote peer in the **Remote Address** field.

  For the example as illustrated in **Figure 3**, the remote site, Site B, has a public IP address of 209.165.200.236. You should choose **Static IP** and enter 209.165.200.236 in the **Remote Address** field.

- **Authentication Method:** Choose one of the following authentication methods:
  - **Pre-shared Key:** Uses a simple, password-based key to authenticate. If you choose this option, enter the desired value that the peer device must provide to establish a connection in the **Key** field. The pre-shared key must be entered exactly the same here and on the remote peer.
  - **Certificate:** Uses the digital certificate from a third party Certificate Authority (CA) to authenticate. If you choose this option, select a CA certificate as the local certificate from the **Local Certificate** drop-down list and select a CA certificate as the remote certificate from the **Remote Certificate** drop-down list. The selected remote certificate on the local gateway must be set as the local certificate on the remote peer.

    NOTE: You must have valid CA certificates imported on your security appliance before choosing this option. Go to the Device Management > Certificate Management page to import the CA certificates. See Managing Certificates for Authentication, page 418.
- **WAN Interface:** Choose the WAN port that traffic passes through over the IPsec VPN tunnel.
- **Local Network:** Choose the IP address for the local network. If you want to configure the zone access control settings for site-to-site VPN, choose **Any** for the local network. Then you can control incoming traffic from remote VPN network to the zones over the VPN tunnels.
- **Remote Network:** Choose the IP address of the remote network. You must know the IP address of the remote network before connecting the VPN tunnel.

  For the example as illustrated in **Figure 3**, Site A has a LAN IP address of 10.10.10.0 and Site B has a LAN IP address of 10.20.20.0. When you configure site-to-site VPN on Site A, the local network is 10.10.10.0 and the remote network is 10.20.20.0.

  If the address object that you want is not in the list, choose **Create a new address** to add a new address object or choose **Create a new address group** to add a new address group object. To maintain the address and address group objects, go to the Networking > Address Management page. See Address Management, page 175.

  NOTE: The security appliance can support multiple subnets for establishing the VPN tunnels. You should select an address group object including multiple subnets for local and/or remote networks.

STEP 4 In the **Advanced Settings** tab, enter the following information:

- **PFS Enable:** Click **On** to enable Perfect Forward Secrecy (PFS) to improve security, or click **Off** to disable it. If you enable PFS, a Diffie-Hellman exchange is performed for every phase-2 negotiation. PFS is desired on the keying channel of the VPN connection.
- **DPD Enable:** Click **On** to enable Dead Peer Detection (DPD), or click **Off** to disable it. DPD is a method of detecting a dead Internet Key Exchange (IKE) peer. This method uses IPsec traffic patterns to minimize the number of messages required to confirm the availability of a peer. DPD is used to reclaim the lost resources in case a peer is found dead and it is also used to perform IKE peer failover. If you enable DPD, enter the following information:
  - **Delay Time:** Enter the value of delay time in seconds between consecutive DPD R-U-THERE messages. DPD R-U-THERE messages are sent only when IPsec traffic is idle. The default value is 10 seconds.
  - **Detection Timeout:** Enter the value of detection timeout in seconds. If no response and no traffic over the timeout, declare the peer dead. The default value is 30 seconds.
  - **DPD Action:** Choose one of the following actions over the detection timeout:

    Hold: Traffic from your local network to the remote network can trigger the security appliance to re-initiate the VPN connection over the detection timeout. We recommend that you use Hold when the remote peer uses a static IP address.

    Clean: Terminate the VPN connection over the detection timeout. You must manually re-initiate the VPN connection. We recommend that you use Clean when the remote peer uses dynamic IP address.

    Restart: Re-initiate the VPN connection for three times over the detection timeout.
- **Windows Networking (NetBIOS) Broadcast:** Click **On** to allow access remote network resources by using its NetBIOS name, for example, browsing Windows Neighborhood. NetBIOS broadcasting can resolve a NetBIOS name to a network address. This option allows NetBIOS broadcasts to travel over the VPN tunnel.
- **Access Control:** When the local network is set as Any, you can control incoming traffic from the remote VPN network to the zones. Click **Permit** to permit access, or click **Deny** to deny access. By default, incoming traffic from the remote network to all zones is permitted.

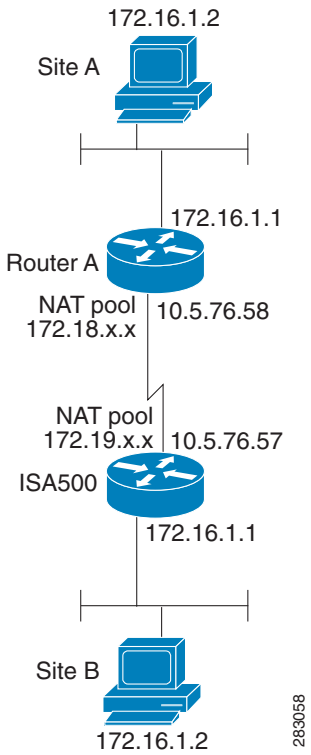
NOTE: The VPN firewall rules that are automatically generated by the zone access control settings will be added to the list of firewall rules with the priority higher than default firewall rules, but lower than custom firewall rules.

- **Apply NAT Policies:** Click **On** to apply the NAT settings for both the local network and the remote network communicating over the VPN tunnel. This option is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
  - **Translates Local Network:** To translate the local network, select a translated address object for the local network.
  - **Translates Remote Network:** To translate the remote network, select a translated address object for the remote network.

  If the address object that you want is not in the list, choose **Create a new address** to add a new address object or choose **Create a new address group** to add a new address group object. To maintain the address or address group objects, go to the Networking > Address Management page. See Address Management, page 175.

  Figure 4 shows a networking example that simulates two merging companies with the same IP addressing scheme. Two routers are connected with a VPN tunnel, and the networks behind each router are the same. For one site to access the hosts at the other site, Network Address Translation (NAT) is used on the routers to change both the source and destination addresses to different subnets.

Figure 4 Networking Example that Simulates Two Merging Companies with the Same IP Addressing Scheme



In this example, when the host 172.16.1.2 at Site A accesses the same IP-addressed host at Site B, it connects to a 172.19.1.2 address rather than to the actual 172.16.1.2 address. When the host at Site B to access Site A, it connects to a 172.18.1.2 address. NAT on Router A translates any 172.16.x.x address to look like the matching 172.18.x.x host entry. NAT on the ISA500 changes 172.16.x.x to look like 172.19.x.x.

NOTE: This configuration only allows the two networks to communicate. It does not allow for Internet connectivity. You need additional paths to the Internet for connectivity to locations other than the two sites; in other words, you need to add another router or firewall on each side, with multiple routes configured on the hosts.

- **IKE Policy:** Choose the IKE policy used for the IPsec VPN policy. You can click **IKE Policy Link** to maintain the IKE policies, but save your settings on this page first.
- **Transform:** Choose the transform set used for the IPsec VPN policy. You can click **Transform Link** to maintain the transform policies, but save your settings on this page first.

- **SA-Lifetime:** Enter the lifetime of the IPsec Security Association (SA). The IPsec SA lifetime represents the interval after which the IPsec SA becomes invalid. The IPsec SA is renegotiated after this interval. The default value is 1 hour.

STEP 5 In the **VPN Failover** tab, enter the following information:

- **WAN Failover Enable:** Click **On** to enable WAN Failover for site-to-site VPN, or click **Off** to disable it. If you enable WAN Failover, the backup WAN port ensures that VPN traffic rolls over to the backup link whenever the primary link fails. The security appliance will automatically update the local WAN gateway for the VPN tunnel based on the configurations of the backup WAN link. For this purpose, Dynamic DNS has to be configured because the IP address will change due to failover, or let the remote gateway use dynamic IP address.

  NOTE: To enable WAN Failover for site-to-site VPN, make sure that the secondary WAN port was configured and the WAN redundancy was set as the Failover or Load Balancing mode.

- **Redundant Gateway:** Click **On** to enable Redundant Gateway, or click **Off** to disable it. If you enable Redundant Gateway, when the connection of the remote gateway fails, the backup connection automatically becomes active. A backup policy comes into effect only if the primary policy fails.

  - **Select Backup Policy:** Choose a policy to act as a backup of this policy.

  - **Fallback Time to switch from back-up to primary:** Enter the number of seconds that must pass to confirm that the primary tunnel has recovered from a failure. If the primary tunnel is up for the specified time, the security appliance will switch to the primary tunnel by disabling the backup tunnel. Enter a value in the range 3 to 59 seconds. The default value is 5 seconds.

    NOTE: DPD should be enabled if you want to use the Redundant Gateway feature for IPsec VPN connection.

STEP 6 Click **OK** to save your settings.

STEP 7 When both the Site-to-Site VPN feature and the IPsec VPN policy are enabled, a warning message appears saying “Do you want to make this connection active when the settings are saved?”

- If you want to immediately activate the connection after the settings are saved, click the **Activate Connection** button. After you save your settings, the security appliance will immediately try to initiate the VPN connection. You can check the Status column to view its connection status.

- If you only want to create the IPsec VPN policy and do not want to immediately activate the connection after the settings are saved, click the **Do Not Activate** button. The connection will be triggered by any traffic that matches the IPsec VPN policy and the VPN tunnel will be set up automatically. You can also click the **Connect** icon to manually establish the VPN connection.

STEP 8 Click **Save** to apply your settings.

Configuring IKE Policies

The Internet Key Exchange (IKE) protocol is a negotiation protocol that includes an encryption method to protect data and ensure privacy. It is also an authentication method to verify the identity of devices that are trying to connect to your network.

You can create IKE policies to define the security parameters (such as authentication of the peer, encryption algorithms, and so forth) to be used for a VPN tunnel.

NOTE Up to 16 IKE policies can be configured on the security appliance.

STEP 1 Click **VPN > Site-to-Site > IKE Policies**.

The IKE Policies window opens. The default and custom IKE policies are listed in the table.

STEP 2 To add a new IKE policy, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**. The default IKE policy (DefaultIke) cannot be edited or deleted.

The IKE Policy - Add/Edit window opens.

STEP 3 Enter the following information:

- **Name:** Enter the name for the IKE policy.
- **Encryption:** Choose the algorithm used to negotiate the security association. There are four algorithms supported by the security appliance: ESP_3DES, ESP_AES_128, ESP_AES_192, and ESP_AES_256.
- **Hash:** Specify the authentication algorithm for the VPN header. There are two hash algorithms supported by the security appliance: SHA1 and MD5.

NOTE: Ensure that the authentication algorithm is configured identically on both sides.

- **Authentication:** Specify the authentication method that the security appliance uses to establish the identity of each IPsec peer.
  - **Pre-shared Key:** Uses a simple, password-based key to authenticate. The alpha-numeric key is shared with the IKE peer. Pre-shared keys do not scale well with a growing network but are easier to set up in a small network.
  - **RSA_SIG:** Uses a digital certificate to authenticate. RSA_SIG is a digital certificate with keys generated by the RSA signatures algorithm. In this case, a certificate must be configured in order for the RSA-Signature to work.
- **D-H Group:** Choose the Diffie-Hellman group identifier, which the two IPsec peers use to derive a shared secret without transmitting it to each other. The D-H Group sets the strength of the algorithm in bits. The lower the Diffie-Hellman group number, the less CPU time it requires to be executed. The higher the Diffie-Hellman group number, the greater the security.
  - Group 2 (1024-bit)
  - Group 5 (1536-bit)
  - Group 14 (2048-bit)
- **Lifetime:** Enter the number of seconds for the IKE Security Association (SA) to remain valid. As a general rule, a shorter lifetime provides more secure ISAKMP (Internet Security Association and Key Management Protocol) negotiations (up to a point). However, with shorter lifetimes, the security appliance sets up future IPsec SAs more quickly. The default value is 24 hours.

STEP 4 Click **OK** to save your settings.

STEP 5 Click **Save** to apply your settings.

Configuring Transform Sets

A transform set specifies the algorithms of integrity and encryption that the peer will use to protect data communications. Two peers must use the same algorithm to communicate.

NOTE Up to 16 transform sets can be configured on the security appliance.

STEP 1 Click **VPN > Site-to-Site > Transform Policies**.

The Transform Sets window opens. The default and custom transform sets are listed in the table.

STEP 2 To add a new transform set, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**. The default transform set (DefaultTrans) cannot be edited or deleted.

The Transform Set - Add/Edit window opens.

STEP 3 Enter the following information:

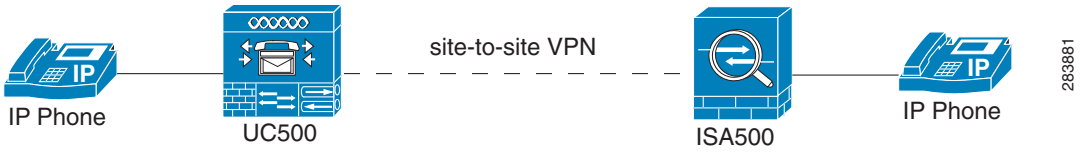
- **Name:** Enter the name for the transform set.
- **Integrity:** Choose the HASH algorithm used to ensure the data integrity. It ensures that a packet comes from where it says it comes from, and that it has not been modified in transit.
  - **ESP_SHA1_HMAC:** Authentication with SHA1 (160-bit).
  - **ESP_MD5_HMAC:** Authentication with MD5 (128-bit). MD5 has a smaller digest and is considered to be slightly faster than SHA1. A successful (but extremely difficult) attack against MD5 has occurred; however, the HMAC variant that IKE uses prevents this attack.
- **Encryption:** Choose the symmetric encryption algorithm that protects data transmission between two IPsec peers. The default is ESP_3DES. The Advanced Encryption Standard supports key lengths of 128, 192, 256 bits.
  - **ESP_3DES:** Encryption with 3DES (168-bit).
  - **ESP_AES_128:** Encryption with AES (128-bit).
  - **ESP_AES_192:** Encryption with AES (192-bit).
  - **ESP_AES_256:** Encryption with AES (256-bit).

STEP 4 Click **OK** to save your settings.

STEP 5 Click **Save** to apply your settings.

Remote Teleworker Configuration Examples

Use Case: You want to establish a site-to-site VPN tunnel between the security appliance and a remote UC500 to provide voice and data services to phones at a remote site.

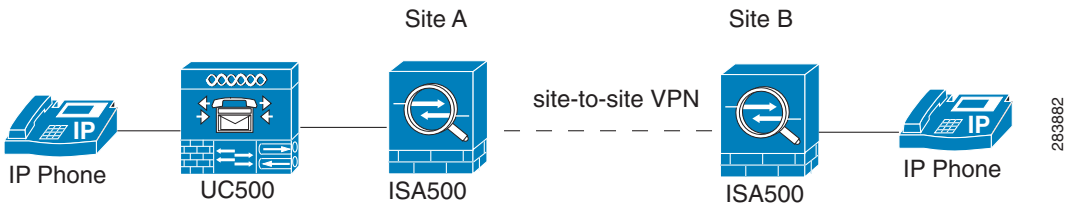


Solution: When you use Cisco Configuration Assistant (CCA) Multisite Manager (MSM) to configure the site-to-site VPN settings on the UC500, CCA MSM uses the default IKE policy and transform set. In this case, the security appliance must create an IPsec VPN policy as follows to establish the site-to-site VPN tunnel with the UC500.

Field	Setting
Remote Network	Choose an address group that includes multiple subnets on the UC500. **NOTE:** By default, three VLANs (192.168.10.0/24, 10.1.1.0/24, and 10.1.10.0/24) are predefined on the UC500.
IKE Policy	Encryption = ESP_3DES Hash = SHA1 D-H Group = Group 2 **NOTE:** The default IKE policy used on the UC500 cannot be modified through CCA. The above IKE settings must be configured on the security appliance.

Field	Setting
Transform	Integrity = ESP_SHA1_HMAC Encryption = ESP_3DES **NOTE:** The default transform set used on the UC500 cannot be modified through CCA. The above transform settings must be configured on the security appliance.

Use Case: The UC500 device is behind the security appliance. You want to establish a site-to-site VPN tunnel between two security appliances to provide voice and data services to phones at a remote site.



Solution: When you configure the site-to-site VPN on the security appliances, make sure that the local network on the security appliance at Site A is set as “Any” and the remote network on the security appliance at Site B is set as “Any”.

Because the security appliance provides the firewall, Network Address Translation (NAT), and SIP Application Level Gateway (SIP ALG) for your network, you must disable those functions on the UC500. For instructions, refer to the documentation or online Help for the Cisco Configuration Assistant (CCA).

To allow the hosts in non-native subnets of the security appliance to access the Internet over the VPN tunnels, you must manually create advanced NAT rules on your security appliance. Go to the Firewall > NAT > Advanced NAT page to do this. For example, you can create an advanced NAT rule as follows to allow the hosts in the data LAN (10.25.1.0/24) behind the UC500 to access the Internet:

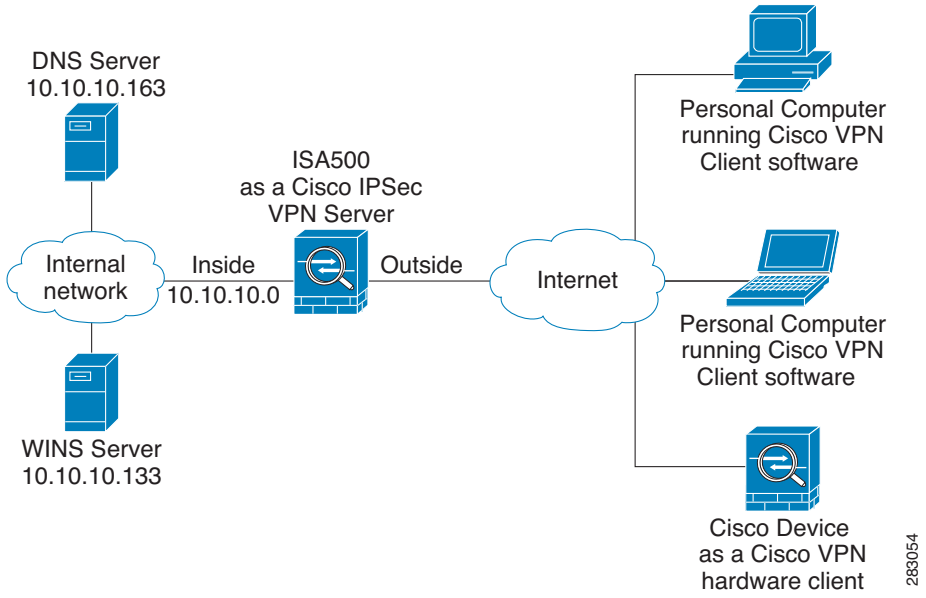
Name	datalan-behinduc500
Enable	On
From	Any
To	WAN1

Original Source Address	uc540-datalan **NOTE:** You can choose the **Create a new address** option from the drop-down list to create an address object for the data LAN (10.25.1.0/24) behind the UC500 and then select it as the original source address.
Original Destination Address	Any
Original Services	Any
Translated Source Address	WAN1_IP
Translated Destination Address	Any
Translated Services	Any

Configuring IPsec Remote Access

The IPsec Remote Access feature introduces server support for the Cisco VPN Client (Release 4.x and 5.x) software clients and the Cisco VPN hardware clients. This feature allows remote users to establish the VPN tunnels to securely access the corporate network resources. Centrally managed IPsec policies are “pushed” to remote VPN clients by the VPN server, minimizing configuration by end users.

Figure 5 IPsec Remote Access with the Cisco VPN Client Software or a Cisco Device as a Cisco VPN Hardware Client



NOTE When the security appliance is acting as an IPsec VPN server, the following IKE policy and transform set are used by default. The IKE policy and transform set used on the security appliance are unconfigurable.

Field	Setting
IKE Policy	Encryption = ESP_AES_256 Hash = SHA Authentication = Pre-shared Key D-H Group = Group 2

Field	Setting
Transform	Integrity = SHA Encryption = ESP_AES_256

This section describes how to configure the IPsec Remote Access feature. Refer to the following topics:

- **Cisco VPN Client Compatibility, page 356**
- **Enabling IPsec Remote Access, page 357**
- **Configuring IPsec Remote Access Group Policies, page 357**
- **Allowing IPsec Remote VPN Clients to Access the Internet, page 360**

Cisco VPN Client Compatibility

The remote VPN client can be a Cisco device acting as a Cisco VPN hardware client or a PC running the Cisco VPN Client software (Release 4.x or 5.x).

The Cisco VPN Client software is an IPsec client software for Windows, Mac, or Linux users. The Cisco VPN Client software is compatible with the following platforms:

- Windows 7 (32-bit and 64-bit)
- Windows Vista (32-bit and 64-bit)
- Windows XP (32-bit)
- Linux Intel (2.6.x kernel)
- Mac OS X 10.5 and 10.6

You can find the software installers for Cisco VPN Client from the CD that is packed with the device. The CD includes the VPN client packages for Windows, Mac OS X, and Linux. Choose correct VPN client package from the CD to download depending on your operating system.

You can also download the Cisco VPN Client software by using this link: http://www.cisco.com/cisco/software/navigator.html?mdfid=278875403 Then choose **Cisco VPN Client**.

NOTE You must log in and possess a valid service contract in order to access the Cisco VPN Client software. A 3-year Cisco Small Business Support Service Contract (CON-SBS-SVC2) is required to download the client software from Cisco.com. If you don't have one, contact your partner or reseller, or Cisco Support for more information.

For more information about how to download, install, and configure the Cisco VPN Client software, see this web page:
http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html

Enabling IPsec Remote Access

STEP 1 Click **VPN > IPsec Remote Access**.

STEP 2 Click **On** to enable the IPsec Remote Access feature and hence set the security appliance as an IPsec VPN server, or click **Off** to disable it.

NOTE: Enabling the IPsec Remote Access feature will disable the Teleworker VPN Client feature.

STEP 3 Click **Save** to apply your settings.

Configuring IPsec Remote Access Group Policies

An IPsec Remote Access group policy is used by remote VPN clients to establish the VPN connections.

NOTE Up to 16 IPsec Remote Access group policies can be configured on the security appliance.

STEP 1 Click **VPN > IPsec Remote Access**.

STEP 2 To add an IPsec Remote Access group policy, click **Add**.

Other Options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The IPsec Remote Access - Add/Edit window opens.

STEP 3 In the **Basic Settings** tab, enter the following information:

- **Group Name:** Enter the name for the group policy.

- **WAN Interface:** Choose the WAN port that traffic passes through over the VPN tunnel.
- **IKE Authentication Method:** Choose the authentication method.
  - **Pre-shared Key:** Uses a simple, password-based key to authenticate. If you choose this option, enter the desired value that remote VPN clients must provide to establish the VPN connections in the **Password** field. The pre-shared key must be entered exactly the same here and on the remote clients.
  - **Certificate:** Uses the digital certificate from a third party Certificate Authority (CA) to authenticate. If you choose this option, select a CA certificate as the local certificate from the **Local Certificate** drop-down list and select a CA certificate as the remote certificate from the **Peer Certificate** drop-down list for authentication. The selected remote certificate on the IPsec VPN server must be set as the local certificate on remote VPN clients.

    NOTE: You must have valid CA certificates imported on your security appliance before choosing this option. Go to the Device Management > Certificate Management page to import the CA certificates. See Managing Certificates for Authentication, page 418.
- **Mode:** The Cisco VPN hardware client supports NEM (Network Extension Mode) and Client mode. The IPsec Remote Access group policy must be configured with the corresponding mode to allow only the Cisco VPN hardware clients in the same operation mode to be connected. For example, if you choose the Client mode for the group policy, only the Cisco VPN hardware clients in Client mode can be connected by using this group policy. For more information about the operation mode, see **Modes of Operation, page 365**.
  - Choose **Client** for the group policy that is used for both the PC running the Cisco VPN Client software and the Cisco device acting as a Cisco VPN hardware client in Client mode. In Client mode, the IPsec VPN server can assign the IP addresses to the outside interfaces of remote VPN clients. To define the pool range for remote VPN clients, enter the starting and ending IP addresses in the **Start IP** and **End IP** fields.
  - Choose **NEM** for the group policy that is only used for the Cisco device acting as a Cisco VPN hardware client in NEM mode.

- **Client Internet Access:** Check this box to automatically create advanced NAT rules to allow remote VPN clients to access the Internet over the VPN tunnels. If you uncheck this box, you can manually create advanced NAT rules. See **Allowing IPsec Remote VPN Clients to Access the Internet, page 360**.
- **WAN Failover:** Click **On** to enable WAN Failover, or click **Off** to disable it. If you enable WAN Failover, traffic is automatically redirected to the secondary link when the primary link is down.

  NOTE: To enable WAN Failover for IPsec Remote Access, make sure that the secondary WAN port was configured and the WAN redundancy was set as the Load Balancing or Failover mode.

  NOTE: The security appliance will automatically update the local WAN gateway for the VPN tunnel based on the configurations of the backup WAN link. For this purpose, Dynamic DNS has to be configured because the IP address will change due to failover and remote VPN clients must use the domain name of the IPsec VPN server to establish the VPN connections.

STEP 4 In the **Zone Access Control** tab, you can control access from the PC running the Cisco VPN Client software or the private network of the Cisco VPN hardware client to the zones over the VPN tunnels. Click **Permit** to permit access, or click **Deny** to deny access.

NOTE: The VPN firewall rules that are automatically generated by the zone access control settings will be added to the list of firewall rules with the priority higher than the default firewall rules, but lower than the custom firewall rules.

STEP 5 In the **Mode Configuration Settings** tab, enter the following information:

- **Primary DNS Server:** Enter the IP address of the primary DNS server.
- **Secondary DNS Server:** Enter the IP address of the secondary DNS server.
- **Primary WINS Server:** Enter the IP address of the primary WINS server.
- **Secondary WINS Server:** Enter the IP address of the secondary WINS server.
- **Default Domain:** Enter the default domain name that should be pushed to remote VPN clients.
- **Backup Server 1/2/3:** Enter the IP address or hostname for the backup server. You can specify up to three IPsec VPN servers as backup. When the connection to the primary server fails, the VPN clients can attempt to connect to the backup servers. The backup server 1 has the highest priority and the backup server 3 has the lowest priority.

NOTE: The backup servers that you specified on the IPsec VPN server will be sent to remote VPN clients when initiating the VPN connections. The remote VPN clients will cache them.

- **Split Tunnel:** Click **On** to enable the split tunneling feature, or click **Off** to disable it. Split tunneling allows only traffic that is specified by the VPN client routes to corporate resources through the VPN tunnel. If you enable split tunneling, you need to define the split subnets. To add a subnet, enter the IP address and netmask in the **Protected Network** and **Netmask** fields and click **Add**. To delete a subnet, select it from the list and click **Delete**.
- **Split DNS:** Split DNS directs DNS packets in clear text through the VPN tunnel to domains served by the corporate DNS. To add a domain, enter the **Domain name** that should be resolved by your network's DNS server, and then click **Add**. To delete a domain, select it from the list and click **Delete**.

  NOTE: To use Split DNS, you must also enable the split tunneling feature and specify the domains. The Split DNS feature supports up to 10 domains.

STEP 6 Click **OK** to save your settings.

STEP 7 Click **Save** to apply your settings.

Allowing IPsec Remote VPN Clients to Access the Internet

Enabling Client Internet Access will automatically create advanced NAT rules to allow remote VPN clients to access the Internet over the VPN tunnels. This section provides an example on manually configuring advanced NAT rules to allow remote VPN clients to access the Internet over the VPN tunnels.

STEP 1 Assuming that you enable the IPsec Remote Access feature and create a group policy as follows:

Field	Setting
Group Name	VPNGroup1
WAN Interface	WAN1
IKE Authentication Method	Pre-shared key

Field	Setting
Mode	Client
Pool Range for Client LAN	Start IP: 192.168.3.2 End IP: 192.168.3.254
Client Internet Access	Disable
WAN Failover	On

NOTE: An address object with the range 192.168.3.2 to 192.168.3.254 called "EZVPN_VPNGroup1" will be automatically created.

STEP 2 If only a single WAN interface is configured, go to the Firewall > NAT > Advanced NAT page to create an advanced NAT rule as follows.

Field	Setting
Name	VPNClient_to_WAN1
Enable	On
From	Any
To	WAN1
Original Source Address	EZVPN_VPNGroup1
Original Destination Address	Any
Original Services	Any
Translated Source Address	WAN1_IP
Translated Destination Address	Any
Translated Services	Any

STEP 3 If two WAN interfaces are configured, go to the Firewall > NAT > Advanced NAT page to create two advanced NAT rules as follows.

Field	Setting
Name	VPNClient_to_WAN1
Enable	On
From	Any
To	WAN1
Original Source Address	EZVPN_VPNGroup1
Original Destination Address	Any
Original Services	Any
Translated Source Address	WAN1_IP
Translated Destination Address	Any
Translated Services	Any

Field	Setting
Name	VPNClient_to_WAN2
Enable	On
From	Any
To	WAN2
Original Source Address	EZVPN_VPNGroup1
Original Destination Address	Any
Original Services	Any
Translated Source Address	WAN2_IP

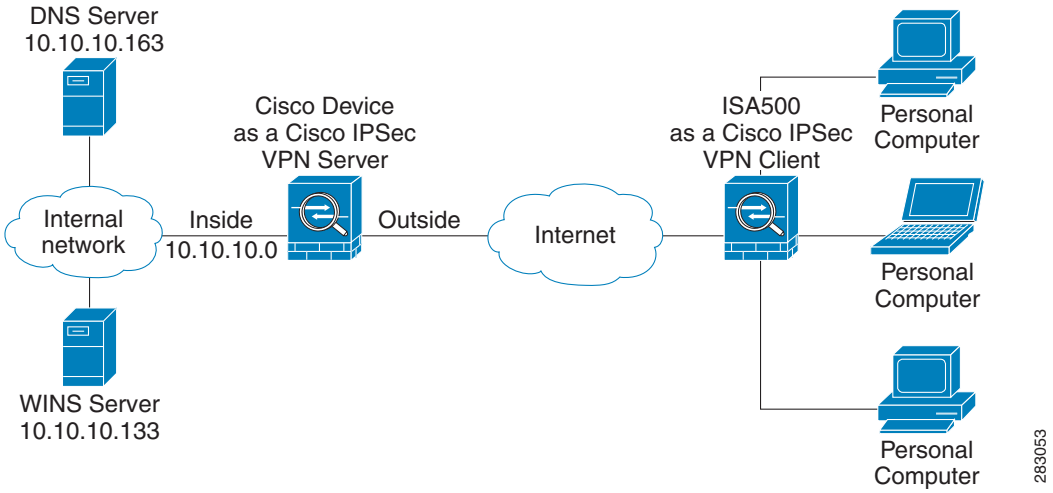
Field	Setting
Translated Destination Address	Any
Translated Services	Any

Configuring Teleworker VPN Client

The Teleworker VPN Client feature minimizes the configuration requirements at remote locations by allowing the security appliance to work as a Cisco VPN hardware client to receive the security policies upon the VPN tunnel from a remote IPsec VPN server.

After the IPsec VPN server has been configured, a VPN connection can be created with minimal configuration on the Teleworker VPN client. When the Teleworker VPN client initiates the VPN connection, the IPsec VPN server pushes the IPsec policies to the Teleworker VPN client and creates the corresponding VPN tunnel. This solution is ideal for remote offices with little IT support or for large Customer Premises Equipment (CPE) deployments where it is impractical to configure multiple remote devices individually.

Figure 6 IPsec Remote Access with an IPsec VPN Server



NOTE When the security appliance is acting as a Cisco VPN hardware client, the following IKE policy and transform set are used by default. The IKE policy and transform set used on the security appliance are unconfigurable.

Field	Setting
IKE Policy	Encryption = ESP_AES_256 Hash = SHA Authentication = Pre-shared Key D-H Group = Group 2
Transform Set	Integrity = SHA Encryption = ESP_AES_256

This section describes how to configure the Teleworker VPN Client feature. Refer to the following topics:

- **Required IPsec VPN Servers, page 364**
- **Benefits of the Teleworker VPN Client Feature, page 365**
- **Modes of Operation, page 365**
- **General Teleworker VPN Client Settings, page 368**
- **Configuring Teleworker VPN Client Group Policies, page 369**

Required IPsec VPN Servers

The Teleworker VPN Client feature requires that the destination peer is an ISA500 device acting as the IPsec VPN server, or a Cisco IOS router (such as C871, C1801, C1812, C1841, and C2821) or a Cisco ASA5500 platform that supports the IPsec VPN server feature.

The Teleworker VPN Client feature supports configuration of only one destination peer. If your application requires multiple VPN tunnels, you must manually configure the VPN tunnel and Network Address Translation/Peer Address Translation (NAT/PAT) parameters on both client and server.

Benefits of the Teleworker VPN Client Feature

- Allows dynamic configuration of end-user policy, requiring less manual configuration by end users and field technicians, thus reducing errors and further service calls.
- Allows the provider to change equipment and network configurations as needed, with little or no reconfiguration of the end-user equipment.
- Provides for centralized security policy management.
- Enables large-scale deployments with rapid user provisioning.
- Eliminates the need for end users to purchase and configure external VPN devices.
- Eliminates the need for end users to install and configure Cisco VPN Client software on their PCs.
- Offloads the creation and maintenance of the VPN connections from the PC to the router.
- Reduces interoperability problems between the different PC-based software VPN clients, external hardware-based VPN solutions, and other VPN applications.
- Sets up a single IPsec tunnel regardless of the number of multiple subnets that are supported and the size of the split-include list.

Modes of Operation

The Teleworker VPN Client feature sets the security appliance as a Cisco VPN hardware client. The Cisco VPN hardware client supports two operation modes: Client Mode or Network Extension Mode (NEM). The operation mode determines whether the inside hosts relative to the Cisco VPN hardware client are accessible from the corporate network over the VPN tunnel. Specifying the operation mode is mandatory before making a connection because the Cisco VPN hardware client does not have a default mode.

All modes of operation also optionally support split tunneling, which allows secure access to corporate resources through the VPN tunnel while also allowing Internet access through a connection to an Internet Service Provider (ISP) or another service—thereby eliminating the corporate network from the path for web access.

Refer to the following topics:

- **Client Mode, page 366**

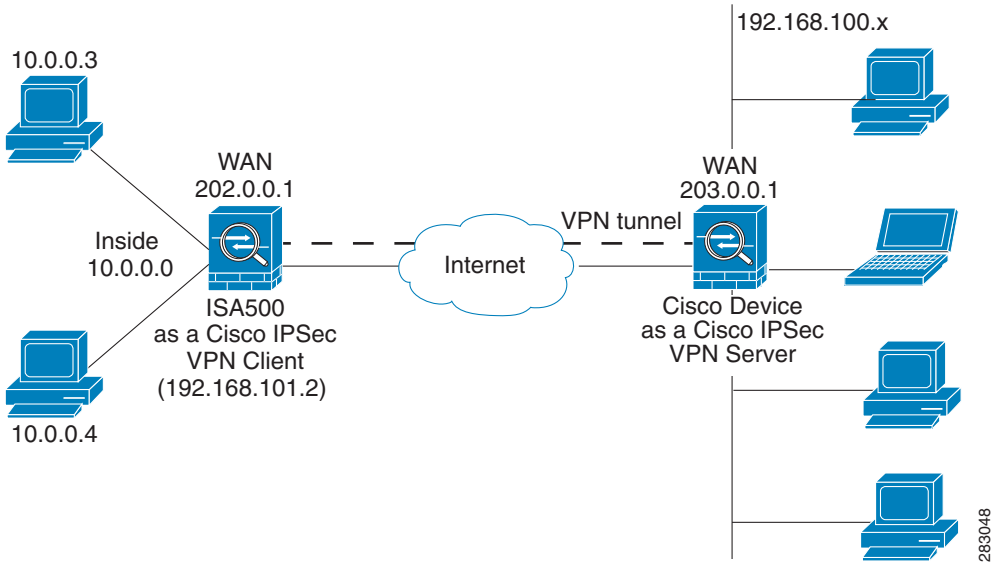
- Network Extension Mode, page 367

Client Mode

Client mode specifies that NAT or PAT be done so that the PCs and other hosts at the remote end of the VPN tunnel form a private network that do not use any IP addresses in the IP address space of the destination server. In Client mode, the outside interface of the Cisco VPN hardware client can be assigned an IP address by the remote server.

Figure 7 illustrates the client mode of operation. In this example, the security appliance provides access to two PCs, which have IP addresses in the 10.0.0.0 private network space. These PCs connect to the Ethernet interface on the security appliance, and the server assigns an IP address 192.168.101.2 to the security appliance. The security appliance performs NAT or PAT translation over the VPN tunnel so that the PCs can access the destination network. When accessing the remote network 192.168.100.x, the hosts 10.0.0.3 and 10.0.04 will be translated to 192.168.101.2, but hosts in the remote network 192.168.100.x cannot access the hosts 10.0.0.3 and 10.0.04.

Figure 7 IPsec VPN Client Connection



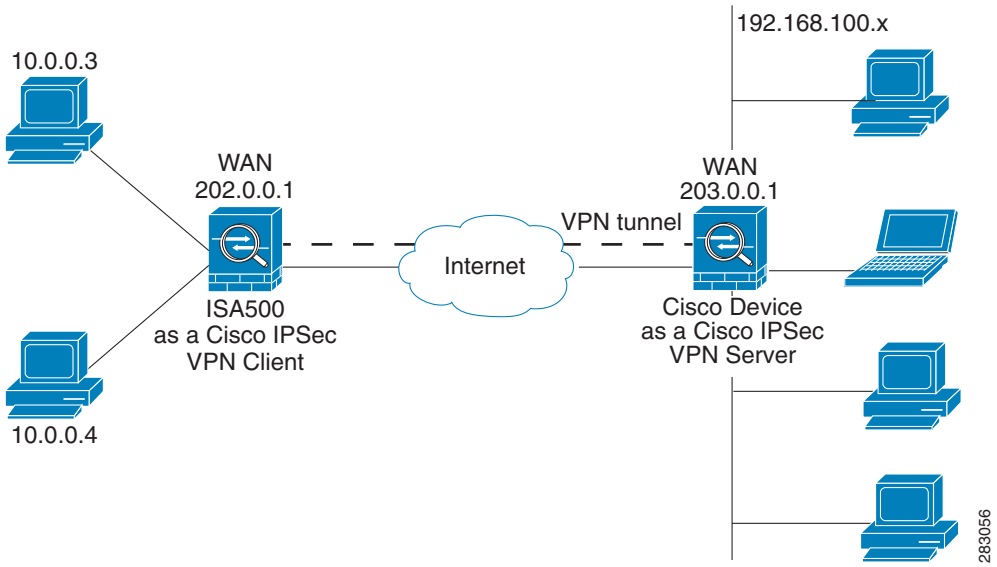
Network Extension Mode

Network Extension Mode (NEM) specifies that the PCs and other hosts at the client end of the VPN tunnel should be given IP addresses that are fully routable and reachable by the destination network over the tunneled network so that they form one logical network. PAT is not used, which allows the client PCs and hosts to have direct access to the PCs and hosts at the destination network. In NEM mode, the Cisco VPN hardware client obtains a private IP address from a local DHCP server or is configured with a static IP address.

Figure 8 illustrates the network extension mode of operation. In this example, the security appliance acts as a Cisco VPN hardware client, connecting to a remote IPsec VPN server. The hosts attached to the security appliance have IP addresses in the 10.0.0.0 private network space. The server does not assign an IP address to the security appliance, and the security appliance does not perform NAT or PAT translation over the VPN tunnel. When accessing the remote network 192.168.100.x, the hosts 10.0.0.3 and 10.0.04 will not be translated, and the hosts in the remote network 192.168.100.x can access the hosts 10.0.0.3 and 10.0.04 directly.

The client hosts are given IP addresses that are fully routable by the destination network over the VPN tunnel. These IP addresses could be either in the same subnet space as the destination network or in separate subnets, assuming that the destination routers are configured to properly route those IP addresses over the VPN tunnel.

Figure 8 IPsec VPN Network Extension Connection



General Teleworker VPN Client Settings

This section describes how to enable the Teleworker VPN Client feature, configure the Auto Initiation Retry settings, and manually connect or disconnect the VPN connections.

STEP 1 Click **VPN > Teleworker VPN Client**.

STEP 2 Enter the following information:

- **Teleworker VPN Client:** Click **On** to enable the Teleworker VPN Client feature and hence set the security appliance as a Cisco VPN hardware client, or click **Off** to disable it.

  NOTE: Enabling the Teleworker VPN Client feature will disable the Site-to-Site VPN and IPsec Remote Access features and terminate their connected VPN sessions.

- **Auto Initiation Retry:** Click **On** to enable the Auto Initiation Retry feature, or click **Off** to disable it.

  When you enable Auto Initiation Retry, the security appliance (set as the Cisco VPN hardware client) first initiates the VPN connection to the primary server. If there is no response from the primary server after the timeout that you set in the **Retry Interval** field, the security appliance then re-initiates the VPN connection to the primary server. This continues for the number of times that you set in the **Retry Limit** field (or until the primary server is connected). If the primary server cannot be connected after the specified number of times, the security appliance tries to re-initiate the VPN connection to the backup servers by following the specified timeout and retry times. If all three backup servers cannot be connected, repeat the re-initiation process again and again until an IPsec VPN server can be connected.

  When you disable Auto Initiation Retry, the security appliance first initiates the VPN connection to the primary server. If there is no response from the primary server in 120 seconds, the security appliance then re-initiates the VPN connection to the backup servers. If all three backup servers cannot be connected, repeat the re-initiation process again and again until an IPsec VPN server can be connected.

- **Retry Interval:** Specify how often, in seconds, that the security appliance re-initiates the VPN connection to the primary server and the back servers. The default value is 120 seconds.

- **Retry Limit:** Enter the number of times that the security appliance will retry a VPN connection initiation. The default value is 2.

STEP 3 Click **Save** to apply your settings.

STEP 4 To manually initiate the VPN connection, click the **Connect** icon in the **Configure** column. By default, the group policy that the Activate Connection on Startup setting is enabled will automatically initiate the VPN connection when the security appliance starts up. Only one VPN connection can be active at a time.

STEP 5 To manually terminate the VPN connection, click the **Disconnect** icon.

Configuring Teleworker VPN Client Group Policies

To be able to complete the configuration of a Teleworker VPN Client group policy, you must have the following information ready.

- IPsec VPN server's IP address or hostname.
- IPsec VPN server's group policy name.
- Pre-shared key or digital certificates for IKE authentication.

NOTE Up to 16 Teleworker VPN Client group policies can be configured on the security appliance. You can create multiple group polices to connect to different VPN servers but only one VPN connection can be active at a time.

STEP 1 Click **VPN > Teleworker VPN Client**.

STEP 2 To add a group policy, click **Add**.

Other Options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The Teleworker VPN Client - Add/Edit window opens.

STEP 3 In the **Basic Settings** tab, enter the following information:

- **Description:** Enter the name for the group policy.
- **Server (Remote Address):** Enter the IP address or domain name of the remote IPsec VPN server.
- **Activate Connection on Startup:** Click **On** to automatically initiate the VPN connection when the security appliance starts up, or click **Off** to disable it. Only one VPN connection can be active on startup.

- **IKE Authentication Method:** The VPN client must be properly authenticated before it can access the remote network. Choose one of the following authentication methods:
  - **Pre-shared Key:** Choose this option if the IPsec VPN server uses a simple, password-based key to authenticate and then enter the following information:

    Group Name: Enter the name of the IPsec Remote Access group policy that is defined on the IPsec VPN server. The security appliance will use this group policy to establish the VPN connection with the IPsec VPN server. The IPsec VPN server pushes the security settings over the VPN tunnel to the security appliance.

    Password: Enter the pre-shared key specified in the selected group policy to establish a VPN connection. The pre-shared key must be entered exactly the same here and on the IPsec VPN server.
  - **Certificate:** Choose this option if the IPsec VPN server uses the digital certificate from a third party Certificate Authority (CA) to authenticate. Select a CA certificate as your local certificate from the **Local Certificate** drop-down list and select the CA certificate used on the remote IPsec VPN server as the remote certificate from the **Peer Certificate** drop-down list for authentication.

    NOTE: You must have valid CA certificates imported on your security appliance before choosing this option. Go to the Device Management > Certificate Management page to import the CA certificates. See Managing Certificates for Authentication, page 418.
- **Mode:** The operation mode determines whether the inside hosts relative to the Cisco VPN hardware client are accessible from the corporate network over the VPN tunnel. Specifying an operation mode is mandatory before making a VPN connection because the Cisco VPN hardware client does not have a default mode. For more information about the operation mode, see **Modes of Operation, page 365**.
  - Choose **Client** if you want the PCs and other devices on the security appliance's inside networks to form a private network with private IP addresses. Network Address Translation (NAT) and Port Address Translation (PAT) will be used. Devices outside the LAN will not be able to ping devices on the LAN, or reach them directly.
  - Choose **NEM** (Network Extension Mode) if you want the devices connected to the inside interfaces to have IP addresses that are routable and reachable by the destination network. The devices at both ends of

the connection will form one logical network. PAT will be automatically disabled, allowing the PCs and hosts at both ends of the connection to have direct access to one another.

- **VLAN:** If you choose NEM, specify the VLAN that permits access from and to the private network of the IPsec VPN server.
- **User Name:** Enter the username used by the Teleworker VPN client to establish a VPN connection.
- **User Password:** Enter the password used by the Teleworker VPN client to establish a VPN connection.

STEP 4 In the **Zone Access Control** tab, you can control access from the zones in your network to the remote network if the Teleworker VPN client works in Client mode. Click **Permit** to permit access, or click **Deny** to deny access.

NOTE: The VPN firewall rules that are automatically generated by the zone access control settings will be added to the list of firewall rules with the priority higher than the default firewall rules, but lower than the custom firewall rules.

STEP 5 In the **Advanced Settings** tab, enter the following information.

- **Backup Server 1/2/3:** Enter the IP address or hostname for the backup server. You can specify up to three servers as backup. When the connection to the primary IPsec VPN server fails, the security appliance can initiate the VPN connection to the backup servers. The backup server 1 has the highest priority and the backup server 3 has the lowest priority.

  NOTE: The Teleworker VPN client can get the backup servers from the IPsec VPN server during the tunnel negotiation. The backup servers specified on the IPsec VPN server have higher priority than the back servers specified on the Teleworker VPN client. When the primary connection fails, first try to connect to the backup servers specified on the IPsec VPN server, and then try to connect to the backup servers specified on the Teleworker VPN client.

- **Peer Timeout:** Enter the value of detection timeout in seconds. If no response and no traffic from the primary server or the backup server over the timeout, declare the peer dead. The default value is 120 seconds.

STEP 6 Click **OK** to save your settings.

STEP 7 A warning message appears saying “Do you want to make this connection active when the settings are saved? (Only one connection can be active at a time.)”

- If you want to immediately activate the connection after the settings are saved, click the **Activate Connection** button. When you create multiple Teleworker VPN Client group policies at a time, only one connection can be active after you save your settings. The security appliance will use the group policy that was last created or edited to initiate the VPN connection.
- If you only want to create the Teleworker VPN client group policy and do not want to immediately activate the connection after the settings are saved, click the **Do Not Activate** button. You can click the **Connect** icon to manually establish the VPN connection.

  NOTE: This feature is different from the Active Connection on Startup feature. It is used to activate the connection immediately after the settings are saved, but the Activate Connection on Startup feature is used to activate the connection when the security appliance starts up.

STEP 8 Click **Save** to apply your settings.

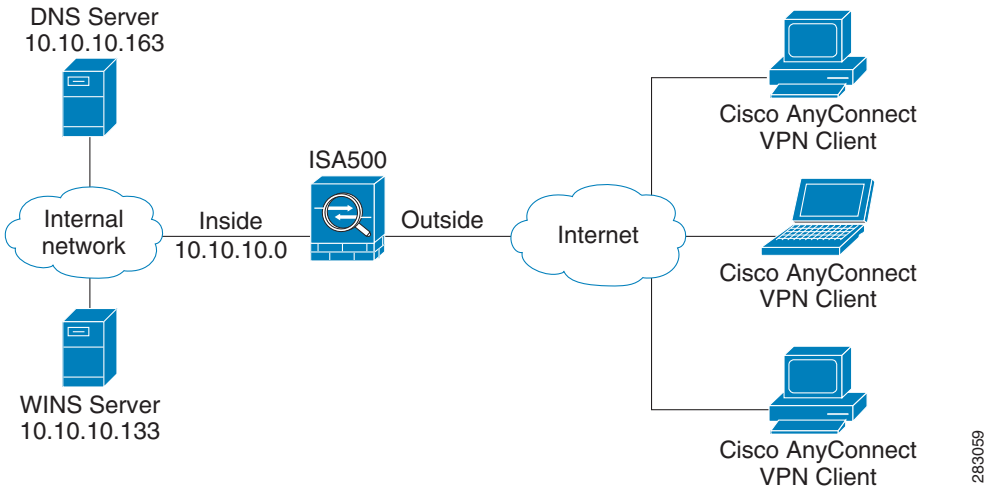
Configuring SSL VPN

SSL VPN is a flexible and secure way to extend network resources to virtually any remote user. The security appliance supports the SSL VPN feature, and interoperates with the Cisco AnyConnect Secure Mobility Client software.

A valid security license is required to support SSLVPN with mobile devices such as smart phones and tablets. For more information, see **Activating Security Services, page 293**.

Figure 9 shows an example of SSL VPN. Users can remotely access the network by using the Cisco AnyConnect Secure Mobility Client software. When the SSL VPN tunnel is established, each user will have an IP address on the internal network.

Figure 9 SSL Remote User Access



This section describes how to configure the SSL VPN feature. Refer to the following topics:

- **Elements of the SSL VPN, page 373**
- **Configuration Tasks to Establish a SSL VPN Tunnel, page 374**
- **Installing Cisco AnyConnect Secure Mobility Client, page 375**
- **Importing Certificates for User Authentication, page 376**
- **Configuring SSL VPN Users, page 376**
- **Configuring SSL VPN Gateway, page 376**
- **Configuring SSL VPN Group Policies, page 379**
- **Accessing SSL VPN Portal, page 382**
- **Allowing SSL VPN Clients to Access the Internet, page 382**

NOTE We do not recommend that you connect a PC or a phone device directly to a WAN port of the security appliance to establish the SSL VPN connection between them.

Elements of the SSL VPN

Several elements work together to support SSL VPN.

- **SSL VPN Users:** Create your SSL VPN users and enable the SSL VPN service for the user groups to which the SSL VPN users belong. Selecting a

SSL VPN group policy can enable the SSL VPN service for a user group. All members of the user group at remote sites can establish the SSL VPN tunnels based on the selected SSL VPN group policy. See **Configuring SSL VPN Users, page 376**.

- **SSL VPN Group Policies:** Create your SSL VPN group policies. The SSL VPN group policy is used to establish the SSL VPN tunnel to access your network resources. See **Configuring SSL VPN Group Policies, page 379**.
- **Cisco AnyConnect Secure Mobility Client:** The Cisco AnyConnect Secure Mobility Client is the next-generation VPN client, providing remote users with secure VPN connections to the SSL VPN gateway. See **Installing Cisco AnyConnect Secure Mobility Client, page 375**.

Configuration Tasks to Establish a SSL VPN Tunnel

You need to complete below configuration tasks to establish the SSL VPN tunnel.

- Download and install the Cisco AnyConnect Secure Mobility Client software on remote user's PC. See **Installing Cisco AnyConnect Secure Mobility Client, page 375**.
- (Optional) Import the certificates to your security appliance used for user authentication. See **Importing Certificates for User Authentication, page 376**.
- Enable the SSL VPN feature and configure the SSL VPN gateway settings. See **Configuring SSL VPN Gateway, page 376**.
- Define the SSL VPN group policies. See **Configuring SSL VPN Group Policies, page 379**.
- Create your SSL VPN users and user groups and specify the SSL VPN group policy for each SSL VPN user group. See **Configuring SSL VPN Users, page 376**.
- Launch the Cisco AnyConnect Secure Mobility Client software on user's PC, enter the address pair "Gateway IP address:Gateway port number" to connect to the remote SSL VPN gateway, and then enter the authentication credentials to establish the SSL VPN connection.
- View information for all active SSL VPN sessions. See **Viewing SSL VPN Status, page 337**.

Installing Cisco AnyConnect Secure Mobility Client

You can set up a PC to run the Cisco AnyConnect Secure Mobility Client software by installing the client software for the appropriate operating system directly on the user's PC. The user starts the Cisco AnyConnect Secure Mobility Client software and provides the authentication credentials to establish the VPN connection.

The security appliance supports the Cisco AnyConnect Secure Mobility Client Release 3.0 (use for SSL only). The Cisco AnyConnect Secure Mobility Client is compatible with the following platforms:

- Windows 7 (32-bit and 64-bit)
- Windows Vista (32-bit and 64-bit)
- Windows XP SP2+ (32-bit and 64-bit)
- Linux Intel (2.6.x kernel)
- Mac OS X 10.5, 10.6.x, and 10.7

You can find the software installers from the CD that is packed with the security appliance. The CD includes AnyConnect packages for Windows, Mac OS X, and Linux. Choose correct AnyConnect package from the CD to download depending on your operating system.

You can also download the Cisco AnyConnect Secure Mobility Client software by going to this site:
http://www.cisco.com/cisco/software/type.html?mdfid=283000185&catid=null

You must log in and possess a valid service contract in order to access the Cisco AnyConnect Secure Mobility Client software. A 3-year Cisco Small Business Support Service Contract (CON-SBS-SVC2) is required to download the client software from Cisco.com. If you don't have one, contact your partner or reseller, or Cisco Support for more information.

For more information about how to download, install, and configure the Cisco AnyConnect Secure Mobility Client software, go to this site:
http://www.cisco.com/en/US/products/ps10884/tsd_products_support_series_home.html

NOTE The Cisco AnyConnect Secure Mobility Client will keep the reconnecting state after the cable of the WAN interface on the server is plugged out and then is plugged in. In this case, you must first stop the client reconnecting, and then manually connect to the SSL VPN server.

Importing Certificates for User Authentication

The SSL VPN gateway holds a CA certificate that is presented to the SSL VPN clients when the SSL VPN clients first connect to the gateway. The purpose of this certificate is to authenticate the server. You can use the default certificate or an imported certificate for authentication. For information on importing the certificates, see **Managing Certificates for Authentication, page 418**.

Configuring SSL VPN Users

ISA550 and ISA550W support 25 SSL VPN users. ISA570 and ISA570W support 50 SSL VPN users. To configure the users and user groups for SSL VPN access, go to the Users > Users and Groups page.

You can assign all SSL VPN users to one user group. However, if you have multiple SSL VPN group policies, you can create multiple user groups and specify different SSL VPN group policies for them. Specifying a SSL VPN group policy for a user group can enable the SSL VPN service for all members of the user group. For complete details, see **Configuring Users and User Groups, page 389**.

According to the user authentication settings specified on the security appliance, the SSL VPN users can be authenticated by the local database or external AAA server (such as Active Directory, LDAP, or RADIUS). For information on configuring the user authentication settings, see **Configuring User Authentication Settings, page 393**.

Configuring SSL VPN Gateway

Use the SSL VPN Configuration page to enable the SSL VPN feature and configure the SSL VPN gateway settings.

STEP 1 Click **VPN > SSL Remote User Access > SSL VPN Configuration**.

The SSL VPN Configuration window opens.

STEP 2 Click **On** to enable the SSL VPN feature and hence set the security appliance as a SSL VPN server, or click **Off** to disable it.

STEP 3 In the **Mandatory Gateway** area, enter the following information:

- **Gateway Interface:** Choose the WAN port that traffic passes through over the SSL VPN tunnels.

- **Gateway Port:** Enter the port number used for the SSL VPN gateway. By default, SSL operates on port 443. However, the SSL VPN gateway should be flexible to operate on a user defined port. The firewall should permit the port to ensure delivery of packets destined for the SSL VPN gateway. The SSL VPN clients need to enter the entire address pair "Gateway IP address: Gateway port number" for connecting purposes.
- **Certificate File:** Choose the default certificate or an imported certificate to authenticate users who try to access your network resource through the SSL VPN tunnels. For information on importing the certificates, see **Managing Certificates for Authentication, page 418**.
- **Client Address Pool:** The SSL VPN gateway has a configurable address pool that is used to allocate IP addresses to remote VPN clients. Enter the IP address pool for all remote clients. The client is assigned an IP address by the SSL VPN gateway.

  NOTE: Configure an IP address range that does not directly overlap with any of addresses on your local network.
- **Client Netmask:** Enter the IP address of the netmask used for SSL VPN clients. The client netmask can only be one of 255.255.255.0, 255.255.255.128, and 255.255.255.192.

  The Client Address Pool is used with the Client Netmask. The following table displays the valid settings for entering the client address pool and the client netmask.

Client Netmask	Client Address Pool
255.255.255.0	x.x.x.0
255.255.255.128	x.x.x.0, or x.x.x.128
255.255.255.192	x.x.x.0, x.x.x.64, x.x.x.128, or x.x.x.192

  If they are set as follows, then the SSL VPN client will get a VPN address whose range is from 10.10.10.1 to 10.10.10.254.

  - Client Address Pool = 10.10.10.0
  - Client Netmask = 255.255.255.0
- **Client Internet Access:** Check this box to automatically create advanced NAT rules to allow SSL VPN clients to access the Internet. If you uncheck this box, you can manually create advanced NAT rules. See **Allowing SSL VPN Clients to Access the Internet, page 382**.

- **Client Domain:** Enter the domain name that should be pushed to SSL VPN clients.
- **Login Banner:** After the users logged in, a configurable login banner is displayed. Enter the message text to display along with the banner.

STEP 4 In the **Optional Gateway** area, enter the following information:

- **Idle Timeout:** Enter the timeout value in seconds that the SSL VPN session can remain idle. The default value is 2100 seconds.
- **Session Timeout:** Enter the timeout value in seconds that a SSL VPN session can remain active. The default value is 0 seconds, which indicates that the SSL VPN session can always be active.
- **Client DPD Timeout:** Dead Peer Detection (DPD) allows detection of dead peers. Enter the DPD timeout that a session will be maintained with a nonresponsive remote client. The default value is 300 seconds.
- **Gateway DPD Timeout:** Enter the DPD timeout that a session will be maintained with a nonresponsive SSL VPN gateway. The default value is 300 seconds.

  NOTE: If the SSL VPN gateway has no response over two or three times of the DPD timeout, the SSL VPN session will be terminated.
- **Keep Alive:** Enter the interval, in seconds, at which the SSL VPN client will send keepalive messages. These messages ensure that the SSL VPN connection remains open, even if the client's maximum idle time is limited by an intermediate device, such as a proxy, firewall or NAT device.
- **Lease Duration:** Enter the amount of time after which the SSL VPN client must send an IP address lease renewal request to the server. The default value is 43200 seconds.
- **Max MTU:** Enter the maximum transmission unit for the session. The default value is 1406 bytes.
- **Rekey Method:** Specify the session rekey method (SSL or New Tunnel). Rekey allows the SSL keys to be renegotiated after the session has been established.
- **Rekey Interval:** Enter the frequency of the rekey in this field. The default value is 3600 seconds.

STEP 5 Click **Save** to apply your settings.

Configuring SSL VPN Group Policies

All members of the SSL VPN user group can establish the SSL VPN tunnels based on the specified SSL VPN group policy to access your network resources.

NOTE Up to 32 SSL VPN group policies can be configured on the security appliance.

STEP 1 Click **VPN > SSL Remote User Access > SSL VPN Group Policies**.

The SSL VPN Group Policies window opens. The default and custom SSL VPN group policies are listed in the table.

STEP 2 To add a new SSL VPN group policy, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**. The default SSL VPN group policy (SSLVPNDefaultPolicy) cannot be deleted.

The SSL VPN Group Policy - Add/Edit window opens.

STEP 3 In the **Basic Settings** tab, enter the following information:

- **Policy Name:** Enter the name for the SSL VPN group policy.
- **Primary DNS:** Enter the IP address of the primary DNS server.
- **Secondary DNS:** Enter the IP address of the secondary DNS server.
- **Primary WINS:** Enter the IP address of the primary WINS server.
- **Secondary WINS:** Enter the IP address of the secondary WINS server.

STEP 4 In the **IE Proxy Settings** tab, enter the following information:

The SSL VPN gateway can specify several Microsoft Internet Explorer (MSIE) proxies for client PCs. If these settings are enabled, IE on the client PC is automatically configured with these settings.

- **IE Proxy Policy:** Choose one of the following IE proxy policies:
  - **None:** Allows the browser to use no proxy settings.
  - **Auto:** Allows the browser to automatically detect the proxy settings.
  - **Bypass-Local:** Allows the browser to bypass the proxy settings that are configured on the remote user.
  - **Disable:** Disables the MSIE proxy settings.

- **Address:** If you choose Bypass-Local or Auto, enter the IP address or domain name of the MSIE proxy server.
- **Port:** Enter the port number of the MSIE proxy server.
- **IE Proxy Exception:** You can specify the exception hosts for IE proxy settings. This option allows the browser not to send traffic for the given hostname or IP address through the proxy. To add an entry, enter the IP address or domain name of an exception host and click **Add**. To delete an entry, select it and click **Delete**.

STEP 5 In the **Split Tunneling Settings** area, enter the following information:

Split tunneling permits specific traffic to be carried outside of the SSL VPN tunnel. Traffic is either included (resolved in tunnel) or excluded (resolved through the ISP or WAN connection). Tunnel resolution configuration is mutually exclusive. An IP address cannot be both included and excluded at the same time.

- **Enable Split Tunneling:** By default, all traffic from the host is directed through the VPN tunnel. Check this box to enable the split tunneling feature so that the VPN tunnel is used only for traffic that is specified by the client routes.
- **Split Selection:** Choose one of the following options:
  - **Include Traffic:** Allows you to add the client routes on the SSL VPN client so that only traffic to the destination networks can be redirected through the VPN tunnel. To add a client route, enter the destination subnet to which a route is added on the SSL VPN client in the **Address** field and the subnet mask for the destination network in the **Netmask** field, and then click **Add**.
  - **Exclude Traffic:** Allows you to exclude the destination networks on the SSL VPN client. Traffic to the destination networks is redirected using the SSL VPN client's native network interface (resolved through the ISP or WAN connection). To add a destination subnet, enter the destination subnet to which a route is excluded on the SSL VPN client in the **Address** field and the subnet mask for the excluded destination in the **Netmask** field, and then click **Add**.

    NOTE: To exclude the destination networks, make sure that the Exclude Local LAN feature is enabled on the Cisco AnyConnect Secure Mobility clients.

- **Exclude Local LAN:** If you choose Exclude Traffic, check the box to permit remote users to access their local LANs without passing through VPN tunnel, or uncheck the box to deny remote users to access their local LANs without passing through VPN tunnel.

  NOTE: To exclude local LANs, make sure that the Exclude Local LAN feature is enabled on both the SSL VPN server and the AnyConnect clients.

- **Split DNS:** Split DNS can direct DNS packets in clear text over the Internet to domains served through an external DNS (serving your ISP) or through the VPN tunnel to domains served by the corporate DNS.

  For example, a query for a packet destined for corporate.com would go through the VPN tunnel to the DNS that serves the private network, while a query for a packet destined for myfavoritesearch.com would be handled by the ISP's DNS. To use Split DNS, you must also have split tunneling configured.

  To add a domain for tunneling packets to destinations in the private network, enter the IP address or domain name in the field and click **Add**. To delete a domain, select it and click **Delete**.

STEP 6 In the **Zone-based Firewall Settings** area, you can control access from the SSL VPN clients to the zones over the VPN tunnels. Click **Permit** to permit access, or click **Deny** to deny access.

NOTE: The VPN firewall rules that are automatically generated by the zone-based firewall settings will be added to the list of firewall rules with the priority higher than the default firewall rules, but lower than the custom firewall rules.

STEP 7 Click **OK** to save your settings.

STEP 8 Click **Save** to apply your settings.

Accessing SSL VPN Portal

The SSL VPN portal provides a message to remind users to install the Cisco AnyConnect Secure Mobility Client software to connect to the SSL VPN server. You can find the software installers from the CD that is packed with the device or download the software installers from Cisco.com. See **Installing Cisco AnyConnect Secure Mobility Client, page 375**.

You can access the SSL VPN portal via a web browser from the WAN side by using the HTTPS protocol. You must first enable the SSL VPN feature on the security appliance and then enter the entire address pair “Gateway IP address:Gateway port number” in the address bar to access the SSL VPN portal.

Allowing SSL VPN Clients to Access the Internet

Enabling Client Internet Access will automatically create advanced NAT rules to allow SSL VPN clients to access the Internet over SSL VPN tunnels. This section provides an example of manually configuring advanced NAT rules to allow SSL VPN clients to access the Internet over SSL VPN tunnels.

STEP 1 Assuming that you enable the SSL VPN feature and configure the gateway settings as follows.

Field	Setting
Gateway Interface	WAN1
Gateway Port	443
Certificate File	default
Client Address Pool	192.168.200.0
Client Netmask	255.255.255.0

STEP 2 If only a single WAN interface is configured, go to the Firewall > NAT > Advanced NAT page to create an advanced NAT rule as follows.

Field	Setting
Name	SSLVPN_to_WAN1

Field	Setting
Enable	On
From	Any
To	WAN1
Original Source Address	SSLVPN_ADDRESS_POOL
Original Destination Address	Any
Original Services	Any
Translated Source Address	WAN1_IP
Translated Destination Address	Any
Translated Services	Any

STEP 3 If two WAN interfaces are configured and the WAN redundancy is set as the Load Balancing mode, go to the Firewall > NAT > Advanced NAT page to create two advanced NAT rule as follows.

Field	Setting
Name	SSLVPN_to_WAN1
Enable	On
From	Any
To	WAN1
Original Source Address	SSLVPN_ADDRESS_POOL
Original Destination Address	Any
Original Services	Any

Field	Setting
Translated Source Address	WAN1_IP
Translated Destination Address	Any
Translated Services	Any

Field	Setting
Name	SSLVPN_to_WAN2
Enable	On
From	Any
To	WAN2
Original Source Address	SSLVPN_ADDRESS_POOL
Original Destination Address	Any
Original Services	Any
Translated Source Address	WAN2_IP
Translated Destination Address	Any
Translated Services	Any

Configuring L2TP Server

Layer 2 Tunneling Protocol (L2TP) is a VPN tunneling protocol that allows remote clients to use the public IP network to securely communicate with private corporate network servers. L2TP uses PPP over UDP (port 1701) to tunnel the data.

L2TP protocol is based on the client and server model. The security appliance can terminate the L2TP-over-IPsec connections from incoming Microsoft Windows clients.

STEP 1 Click **VPN > L2TP Server**.

STEP 2 Click **On** to enable L2TP server, or click **Off** to disable it.

STEP 3 If you enable L2TP server, enter the following information:

- **Listen WAN Interface:** Choose the WAN interface on which the L2TP server listens to accept the incoming L2TP VPN connection.
- **User Name:** Enter the username that all L2TP clients use to access the L2TP server.
- **Password:** Enter the password that all L2TP clients use to access the L2TP server.

  NOTE: All L2TP clients use the same username and password to log into the L2TP server.
- **MTU:** Enter the MTU size in bytes that can be sent over the network. The valid range is 128 to 1400 bytes. The default value is 1400 bytes.
- **Authentication Method:** Choose either CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol), or both to authenticate the L2TP clients. Click **On** to enable CHAP or PAP, or click **Off** to disable it.
- **Address Pool:** The L2TP server assigns IP addresses to all L2TP clients. Enter the starting IP address in the **Start IP Address** field and the ending IP address in the **End IP Address** field.
- **DNS1 IP Address:** Enter the IP address of the primary DNS server.
- **DNS2 IP Address:** Optionally, enter the IP address of the secondary DNS server.

- **IPsec:** Click **On** to enable the data encryption over the IPsec VPN tunnel, or click **Off** to disable it.
- **Pre-shared Key:** The data encryption over the VPN tunnel uses a pre-shared key for authentication. If you enable **IPsec**, enter the desired value, which the L2TP client must provide to establish a connection. The pre-shared key must be entered exactly the same here and on the L2TP clients.

STEP 4 Click **Save** to apply your settings.

STEP 5 By default, the firewall denies access from VPN zone to LAN and voice zones. If you want to allow L2TP clients to access your default VLAN, you must go to the Firewall > Access Control > ACL Rules page to manually create a firewall rule as follows:

Field	Setting
From Zone	VPN
To Zone	LAN
Service	Any
Source Address	l2tp_clients **NOTE:** Choose **Create a new address** from the drop-down list to create an address object "l2tp_clients" with the IP address range of L2TP server's address pool.
Destination Address	DEFAULT_NETWORK
Schedule	Always on
Match Action	Permit

Configuring VPN Passthrough

Use the VPN Passthrough page to configure VPN Passthrough to allow VPN traffic that originates from VPN clients to pass through your security appliance. Use this feature if there are devices behind your security appliance that need the IPSec tunnels to be set up independently, such as connecting to another router on the WAN.

STEP 1 Click **VPN > VPN Passthrough**.

The VPN Passthrough window opens.

STEP 2 Specify the type of traffic that can pass through the security appliance:

- **Layer-2 Tunneling Protocol (L2TP):** Click **On** to allow L2TP tunnels to pass through the security appliance, or click **Off** to disable it.
- **Point-to-Point Tunneling Protocol (PPTP):** Click **On** to allow PPTP tunnels to pass through the security appliance, or click **Off** to disable it.
- **Internet Protocol Security (IPsec):** Click **On** to allow IP security tunnels to pass through the security appliance, or click **Off** to disable it.

STEP 3 Click **Save** to apply your settings.

9

User Management

This chapter describes how to manage users, user groups, and configure user authentication settings. It includes the following sections:

- **Viewing Active User Sessions, page 388**
- **Configuring Users and User Groups, page 389**
- **Configuring User Authentication Settings, page 393**
- **Configuring RADIUS Servers, page 401**

To access the Users pages, click **Users** in the left hand navigation pane.

Viewing Active User Sessions

Use the Active User Sessions page to view information for all active user sessions that are currently logged into the security appliance. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data. Click the **Logout** icon to terminate a web login user session or a VPN user session.

Users > Active User Sessions

Field	Description
User Name	Name of the logged user.
IP Address	Host IP address from which the user accessed the security appliance.
Login Method	How the user logs into the security appliance, such as WEB, SSL VPN, IPsec Remote Access, or Captive Portal.
Session Time	Time that the user has logged into the security appliance.

Configuring Users and User Groups

This section describes how to maintain the users and user groups in local database. Refer to the following topics:

- **Default User and User Group, page 389**
- **Available Services for User Groups, page 389**
- **Preempt Administrators, page 390**
- **Configuring Local Users, page 390**
- **Configuring Local User Groups, page 391**

Default User and User Group

The security appliance maintains user and user group information in the local database. The local database supports up to 100 users and 50 user groups. A user group can include up to 100 users. Any user must be a member of a user group.

The default administrator account (“cisco”) has full privilege to set the configuration and read the system status. The default administrator account cannot be deleted. For security purposes, you must change the default administrator password at the first login. See Changing the Default Administrator Password, page 32.

The default user group (“admin”) has the administrative web login access ability and enables the SSL VPN, IPsec Remote Access, and Captive Portal services. The default user group cannot be deleted, but its service policy can be modified.

Available Services for User Groups

A user can only belong to one user group. The users in the same user group share the same service policy. A user group has only one service policy. The services available for a user group include:

- **Web Login:** Allows the members of the user group to log into the Configuration Utility through the web browser to view the configuration only or to set the configuration.
- **SSL VPN:** Allows the members of the user group at remote sites to establish the SSL VPN tunnels based on the selected SSL VPN group

policy to access your network resources. The Cisco AnyConnect Secure Mobility Client software must be installed on user's PC.

- **IPsec Remote Access:** Allows the members of the user group at remote sites to establish the VPN tunnels to securely access your network resources.
- **Captive Portal:** Allows the wireless users who have authenticated successfully to be directed to a specified web page (portal) before they can access the Internet. This service only applies to ISA550W and ISA570W.

NOTE The security appliance can perform the authentications in parallel when multiple services need to authenticate at the same time.

Preempt Administrators

When an administrator attempts to log in while another administrator is logged in, a warning message appears saying "Another administrative user is logged into the application. Do you want to take control of the session? (The other user will be logged out.)" Click **Yes** to preempt the current administrator, or click **No** to return to the login screen.

Configuring Local Users

Use the Users and Groups page to view, add, edit, or delete local users. The local database supports up to 100 users.

STEP 1 Click **Users > Users and Groups**.

The Users and Groups window opens. All existing local users are listed in the Local Users table.

STEP 2 In the **Local Users** area, click **Add** to add a user.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The Local User - Add/Edit window opens.

STEP 3 Enter the following information:

- **User:** Enter the username for the user.
- **New Password:** Enter the password for the user. Passwords are case sensitive.

  NOTE: A password requires a minimum of 8 characters, including at least three of these character classes: uppercase letters, lowercase letters, digits, and special characters. Do not repeat any password more than three times in a row. Do not set the password as the username or "cisco." Do not capitalize or spell these words backwards.
- **New Password Confirm:** Enter the password again for confirmation.
- **Group:** Choose the user group to which the user belongs.

  NOTE: For a SSL VPN user, make sure that the selected user group enables the SSL VPN service. For an IPsec VPN user, make sure that the selected user group enables the IPsec Remote Access service.

STEP 4 Click **OK** to save your settings.

Configuring Local User Groups

A user group is used to create a logical grouping of users that share the same service policy. Use the Users and Groups page to view, add, edit, or delete local user groups. The local database supports up to 50 user groups.

STEP 1 Click **Users > Users and Groups**.

The Users and Groups window opens. All existing user groups are listed in the Groups table.

STEP 2 In the **Groups** area, click **Add** to add a user group.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The Group - Add/Edit window opens.

STEP 3 In the **Group Settings** tab, enter the following information:

- **Name:** Enter the name for the user group.
- **Services:** Specify the service policy for the user group. You can enable multiple services for a user group.
  - **Web Login:** Choose one of the following web login policies for the user group.

    Disable: All members of the user group cannot log into the Configuration Utility through the web browser.

    Read Only: All members of the user group can only read the system status after they login. They cannot edit any configuration.

    Administrator: All members of the user group have full privilege to set the configuration and read the system status.

    NOTE: You cannot disable the web login service or change its service level for the default user group (“admin”).
  - **SSL VPN:** Choose a SSL VPN group policy to enable the SSL VPN service for the user group, or choose **Disable** to disable it. If you enable SSL VPN, all members of the user group can establish the SSL VPN tunnels based on the selected SSL VPN group policy to securely access your network resources. For more information about the SSL VPN group policy, see Configuring SSL VPN Group Policies, page 379.
  - **IPsec Remote Access:** Click **Enable** to enable the IPsec Remote Access service for the user group, or click **Disable** to disable it. If you enable IPsec Remote Access, all members of the user group can establish the VPN tunnels to securely access your network resources.
  - **Captive Portal:** Click **Enable** to enable the Captive Portal service for the user group, or click **Disable** to disable it. If you enable Captive Portal, the members of the user group will be directed to a specified web page (portal) before they can access the Internet. To configure Captive Portal, see Configuring Captive Portal, page 221,.

STEP 4 In the **Membership** tab, specify the members of the user group.

- To add a member, select an existing user from the **User** list and click the right arrow. The members of the user group appear in the **Membership** list.
- To delete a member from the user group, select the user from the **Membership** list and click the left arrow.

STEP 5 Click **OK** to save your settings.

Configuring User Authentication Settings

User authentication is a means of identifying the user and verifying that the user is allowed to access some restricted services. For example, a user can be identified as a SSL VPN user in order to access your network resources over SSL VPN tunnels.

The security appliance authenticates all users when they attempt to access your network resources in different zones. Users on the VLANs perform only local tasks, and are not required to be authenticated by the security appliance.

The security appliance supports a local database that is stored on the security appliance and a variety of AAA server types, such as RADIUS, Lightweight Directory Access Protocol (LDAP), and Active Directory (AD). You can use the local database, an AAA server, or both to perform user authentication. The local database supports up to 100 users, so you need to use the AAA server for authentication if the number of users accessing the network is more than 100 users.

NOTE The user group service policy can only be configured locally. All user groups on an AAA server need to be duplicated locally.

Refer to the following topics:

- **Using Local Database for User Authentication, page 394**
- **Using RADIUS Server for User Authentication, page 394**
- **Using Local Database and RADIUS Server for User Authentication, page 397**
- **Using LDAP for User Authentication, page 398**
- **Using Local Database and LDAP for Authentication, page 400**

Using Local Database for User Authentication

Use the local database to authenticate users when the number of users accessing the network is less than 100 users.

The local database verifies the user's credentials. Only the valid local users are allowed to access the network. For information on configuring local users in the local database, see **Configuring Local Users, page 390**.

STEP 1 Click **Users > User Authentication**.

STEP 2 Choose **Local Database** as the authentication method.

STEP 3 Click **Save** to apply your settings.

Using RADIUS Server for User Authentication

The security appliance can use RADIUS servers for user authentication for network access. The RADIUS server uses the Framed-Filter-ID attribute to store user and user group information, and checks the user's credentials by using the Password Authentication Protocol (PAP) authentication scheme.

When a user authenticates, the security appliance verifies the user's credentials through the RADIUS server. The RADIUS server returns the authentication results to the security appliance. For a valid RADIUS user, the security appliance checks its user group service policy from the local database and permits access. For an invalid RADIUS user, the security appliance blocks access.

STEP 1 Click **Users > User Authentication**.

STEP 2 Choose **RADIUS** as the authentication method.

STEP 3 Click **Configure** to configure the RADIUS settings.

STEP 4 In the **Settings** tab, choose the RADIUS group for authentication and configure the global timeout and retry settings.

- **Global RADIUS Settings:** Specify the global timeout and retry settings for the selected RADIUS servers:
  - **RADIUS Server Timeout:** Enter the number of seconds that the connection can exist before re-authentication is required. The range is 1-60 seconds. The default value is 3 seconds.

- **Retries:** Enter the number of times that the security appliance will try to contact the RADIUS server. The range is 0-10 attempts. The default value is 2.

The security appliance first sends a request message to the primary RADIUS server. If there is no response from the primary RADIUS server, the security appliance waits the number of seconds that you set in the **RADIUS Server Timeout** field, and then sends another request message. This continues for the number of times that you set in the **Retries** field (or until there is a valid response). If there is no valid response from the primary RADIUS server after the specified number of retries, the security appliance uses the secondary RADIUS server for the next authentication attempt. If the secondary server also fails to respond after the specified number of retries, the connection is dropped.

- **RADIUS Servers:** Choose the RADIUS group index from the drop-down list. The RADIUS server settings of the selected group are displayed. You can edit these settings here but the settings you specify will replace the default settings of the selected group. To maintain the RADIUS server settings, go to the Users > RADIUS Servers page. See **Configuring RADIUS Servers, page 401**.

STEP 5 In the **RADIUS Users** tab, enter the following information:

- **Allow Only Users Listed Locally:** Click **On** to allow only the RADIUS users who also are present in the local database to login, or click **Off** to disable it.
- **Mechanism for Setting User Group Memberships for RADIUS Users:** Select one of the following mechanisms to configure the user group memberships for RADIUS users:
  - **Use RADIUS Filter-ID:** Find the user group information by using the Framed-Filter-ID attribute from the RADIUS server.

    For example, the RADIUS server has three user groups (Group1, Group2, and Group3) and the local database has two user groups (Group1 and Group2). The following table displays the user group membership settings.

Local Database Settings	**RADIUS Server Settings**		
	User1 in Group1	User1 in Group2	User1 in Group3

User1 in Group1	Group1	Group2	Default Group
User1 in Group2	Group1	Group2	Default Group
User1 does not exist	Group1	Group2	Default Group

In the above table, if the User1 in the RADIUS server belongs to the Group1 but the User1 in the local database belongs to the Group2, then the User1 will belong to the Group1 after the user passes the RADIUS authentication. If the User1 in the RADIUS server belongs to the Group3 but the local database has not the Group3, then the User1 will be set to the specified default group.

- **Local Configuration Only:** Find the user group information from the local database only.

  For example, the RADIUS server has three user groups (Group1, Group2, and Group3) and the local database has two user groups (Group1 and Group2). The following table displays the user group membership settings.

Local Database Settings	**RADIUS Server Settings**		
	User1 in Group1	User1 in Group2	User1 in Group3
User1 in Group1	Group1	Group1	Group1
User1 in Group2	Group2	Group2	Group2
User1 does not exist	Default Group	Default Group	Default Group

In the above table, if the User1 in the RADIUS server belongs to the Group1 but the User1 in the local database belongs to the Group2, then the User1 will belong to the Group2 after the user passes the RADIUS authentication. If the User1 does not exist in the local database, it will be set to the specified default group.

- **Default User Group to Which All RADIUS Users Belong:** Choose a local user group as the default group to which the RADIUS users belong. If the group does not exist in the local database when getting user group information from the RADIUS server, the RADIUS user will be automatically set to the specified local user group.

STEP 6 In the **Test** tab, enter the user's credentials in the **User** and **Password** fields, and then click the **Test** button to verify whether the RADIUS user is valid.

STEP 7 Click **OK** to save your settings.

STEP 8 Click **Save** to apply your settings.

Using Local Database and RADIUS Server for User Authentication

You can use both the local database and RADIUS server to authenticate users who try to access the network.

When a user authenticates, the security appliance first verifies the user's credentials through the RADIUS server. The RADIUS server returns the authentication results to the security appliance. For a valid RADIUS user, the security appliance checks its user group service policy from the local database and permits access. For an invalid RADIUS user, then the security appliance uses the local database to verify it again. For a valid local user, the security appliance checks its user group service policy from the local database and permits access. For an invalid local user, the security appliance blocks access.

STEP 1 Click **Users > User Authentication**.

STEP 2 Choose **RADIUS + Local Database** as the authentication method.

STEP 3 Click **Configure** to configure the RADIUS settings for user authentication. For complete details, see **Using RADIUS Server for User Authentication, page 394**.

STEP 4 Click **Save** to apply your settings.

Using LDAP for User Authentication

The security appliance can use the LDAP directory for user authentication, with support of three schemes including Microsoft Active Directory, RFC2798 InterOrgPerson, and RFC2307 Network Information Service.

STEP 1 Click **Users > User Authentication**.

STEP 2 Choose **LDAP** as the authentication method.

STEP 3 Click **Configure** to configure the LDAP settings.

STEP 4 In the **Settings** tab, enter the following information:

- **IP Address:** Enter the IP address of the LDAP server.
- **Port Number:** Enter the listening IP port number used on the LDAP server. Typically, non-secure connections use 389 and secure connections use 636. The default is 389.
- **Server Timeout:** Enter the amount of time in seconds that the security appliance will wait for a response from the LDAP server before timing out. The default value is 5 seconds.

  The security appliance will retry to log in to the LDAP server if there is no response from the LDAP server after the timeout. For example, if the server timeout is set as 5 seconds and there is no response from the LDAP server after 5 seconds, the security appliance will then retry to log in to the LDAP server 5 seconds later.
- **Login Method:** Choose one of the following login methods:
  - **Anonymous Login:** Choose this option if the LDAP server allows for the user tree to be accessed anonymously.
  - **Give Login Name or Location in Tree:** Choose this option if the distinguished name that is used to bind to the LDAP server is built from the **Primary Domain** and **User Tree for Login to Server** fields in the **Directory** tab.
  - **Give Bind Distinguished Name:** Choose this option if the destination name is known. You must provide the destination name explicitly to be used to bind to the LDAP server.
- **Login User Name:** If you choose **Give Login Name or Location in Tree** or **Give Bind Distinguished Name** as the login method, enter the user distinguished name of the account that can log into the LDAP server.

- **Login Password:** If you choose **Give Login Name or Location in Tree** or **Give Bind Distinguished Name** as the login method, enter the password of the account that can log into the LDAP server.
- **Protocol Version:** Choose the LDAP version from the drop-down list. The security appliance supports LDAP Version 2 and LDAP Version 3. Most LDAP directories, including Active Directory, use LDAP Version 3.

STEP 5 In the **Schema** tab, enter the following information:

- **LDAP Schema:** Choose one of the following schemes:
  - Microsoft Active Directory
  - RFC2798 InetOrgPerson
  - RFC2307 Network Information Service
- **User Objects:** The following fields display their correct values used by the selected scheme. The fields that are grayed out cannot be edited, but you can specify the editable fields if you have a specific LDAP scheme configuration.
  - **Object Class:** The object class of the individual user account.
  - **Login Name Attribute:** The attribute that is used for login authentication.
  - **Qualified Login Name Attribute:** The attribute of a user object that sets an alternative login name for the user in name@domain format.
  - **User Group Membership Attribute:** The membership attribute that contains information about the group to which the user object belongs. This option is only available for Microsoft Active Directory.
  - **Framed IP Address Attribute:** The attribute to retrieve a static IP address that is assigned to a user in the directory.
- **User Group Objects:** The following fields display their correct values used by the selected scheme.
  - **Object Class:** The name associated with the group of attributes.
  - **Member Attribute:** The attribute associated with a member.

STEP 6 In the **Directory** tab, enter the user direction information in the following fields:

- **Primary Domain:** Enter the user domain used by your LDAP implementation. All domain components use “dc=”. The domain is formatted as “dc=ExampleCorporation, dc=com”.

- **User Tree for Login to Server:** If you choose **Give Login Name or Location in Tree** as the login method in the **Settings** tab, specify the user tree that is used to log into the LDAP server.
- **Trees Containing Users:** Specify the user trees in the LDAP directory. To add an entry, click **Add**. To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click **Remove**. To modify the priority of an entry in the tree, click the up arrow or the down arrow.
- **Trees Containing User Groups:** Specify the user trees in the LDAP directory. These are only applicable when there is no user group membership attribute in the scheme's user object, and are not used with AD. To add an entry, click **Add**. To edit an entry, click **Edit**. To delete an entry, click **Remove**. To modify the priority of an entry in the tree, click the up arrow or the down arrow.

  NOTE: All the above trees are given in the format of distinguished names ("cn=Users, dc=ExampleCorporation, dc=com").

STEP 7 In the **LDAP Users** tab, enter the following information:

- **Allow Only Users Listed Locally:** Click **On** to allow only the LDAP users who also are present in the local database to login, or click **Off** to disable it.
- **Default LDAP User Group:** Choose a local user group as the default group to which the LDAP users belong. If the group does not exist in the local database when getting user group information from the LDAP server, the LDAP user will be automatically set to the specified local user group.

STEP 8 In the **Test** tab, enter the user's credentials in the **User** and **Password** fields and then click **Test** to verify whether the LDAP user is valid.

STEP 9 Click **OK** to save your settings.

STEP 10 Click **Save** to apply your settings.

Using Local Database and LDAP for Authentication

You can use both the local database and LDAP to authenticate users who try to access to the network.

STEP 1 Click **Users > User Authentication**.

STEP 2 Choose **LDAP + Local Database** as the authentication method.

STEP 3 Click **Configure** to configure the LDAP settings for user authentication. For complete details, see **Using LDAP for User Authentication, page 398**.

STEP 4 Click **Save** to apply your settings.

Configuring RADIUS Servers

Use the RADIUS Servers page to configure the RADIUS servers that are used to authenticate users who try to access the network resources. A RADIUS group includes a primary RADIUS server and a backup RADIUS server. The security appliance predefines three RADIUS groups.

STEP 1 Click **Users > RADIUS Servers**.

The RADIUS Servers window opens. All predefined RADIUS groups are listed in the table.

STEP 2 To edit the settings for a predefined RADIUS group, click the **Edit** (pencil) icon.

The RADIUS Group - Edit window opens.

STEP 3 Enter the following information:

- **Primary RADIUS Server IP:** Enter the IP address of the primary RADIUS server.
- **Primary RADIUS Server Port:** Enter the port number on the primary RADIUS server that is used to send the RADIUS traffic. The default is 1812.
- **Primary RADIUS Server Pre-shared Key:** Enter the pre-shared key that is configured on the primary RADIUS server.
- **Secondary RADIUS Server IP:** Enter the IP address of the secondary RADIUS server.
- **Secondary RADIUS Server Port:** Enter the port number on the secondary RADIUS server that is used to send the RADIUS traffic. The default is 1812.
- **Secondary RADIUS Server Pre-shared Key:** Enter the pre-shared key that is configured on the secondary RADIUS server.

STEP 4 Click **OK** to save your settings.

STEP 5 Repeat the above steps to edit the settings for other RADIUS groups if needed.

STEP 6 Click **Save** to apply your settings.

10

Device Management

This chapter describes how to maintain the configuration and firmware, reboot or reset the security appliance, manage the security license and digital certificates, and configure other features to help maintain the security appliance. It includes the following sections:

- Viewing System Status, page 404
- Administration, page 405
- Backing Up and Restoring a Configuration, page 416
- Managing Certificates for Authentication, page 418
- Configuring Cisco Services and Support Settings, page 424
- Backing Up and Restoring a Configuration, page 416
- Configuring System Time, page 427
- Configuring Device Properties, page 428
- Diagnostic Utilities, page 428
- Device Discovery Protocols, page 430
- Firmware Management, page 434
- Managing Security License, page 439
- Log Management, page 442
- Rebooting and Resetting the Device, page 448
- Configuring Schedules, page 449

To access the Device Management pages, click **Device Management** in the left hand navigation pane.

Viewing System Status

This section describes how to view information for all running processes and the system's CPU and memory utilization. Refer to the following topics:

- Viewing Process Status, page 404
- Viewing Resource Utilization, page 404

Viewing Process Status

Use the Processes page to view information for all running processes. This page is automatically updated every 10 seconds. Click **Refresh** to manually refresh the data.

Device Management > System Status > Processes

Field	Description
Name	Name of the process that is running on the security appliance.
Description	Brief description for the running process.
Protocol	Protocol that is used by the socket.
Port	Port number of the local end of the socket.
Local Address	IP address of the local end of the socket.
Foreign Address	IP address of the remote end of the socket.

Viewing Resource Utilization

Use the Resource Utilization page to view information for the system's CPU and memory utilization.

Device Management > System Status > Resource Utilization

Field	Description
CPU Utilization	
CPU Usage by User	CPU resource currently used by user space processes, in percentage.

Field	Description
CPU Usage by Kernel	CPU resource currently used by kernel space processes, in percentage.
CPU Idle	CPU idle resource at current time, in percentage.
CPU Waiting for I/O	CPU resource currently waiting for I/O, in percentage.
Memory Utilization	
Total Memory	Total amount of memory space available on the security appliance.
Memory Used	Total amount of memory space currently used by the processes.
Free Memory	Total amount of memory space currently not used by the processes.
Cached Memory	Total amount of memory space currently used as cache.
Buffer Memory	Total amount of memory space currently used as buffers.

Administration

Use the Administration pages to modify the username and password for the default administrator account, configure the user session settings, centrally configure the email alert settings, and configure remote management and SNMP.

This section includes the following topics:

- **Configuring Administrator Settings, page 406**
- **Configuring Remote Administration, page 407**
- **Configuring Email Alert Settings, page 408**
- **Configuring SNMP, page 415**

Configuring Administrator Settings

Use the Administrator Settings page to modify the username and password for the default administrator account and configure the user session settings. The user session settings are applicable for all authentication methods.

NOTE At your first login, you must change the default administrator password for security purposes. The Administrator Settings page provides another approach to modify the username and password for the default administrator account, but not for the first login.

STEP 1 Click **Device Management > Administration > Administrator Settings**.

STEP 2 To update your password, enter the following information in the **Administrator Name and Password** area:

- **User Name:** Enter the current username of the default administrator account, or enter a new username if you want to change it.
- **Current Password:** Enter the current administrator password.
- **New Password:** Enter a new administrator password. Passwords are case sensitive.

  NOTE: A password requires a minimum of 8 characters, including at least three of these character classes: uppercase letters, lowercase letters, digits, and special characters. Do not repeat any password more than three times in a row. Do not set the password as the username or “cisco.” Do not capitalize or spell these words backwards.
- **Confirm New Password:** Enter the new password again for confirmation.

STEP 3 To modify the user session settings, enter the following information in the **Session** area:

- **Inactivity Timeout:** Enter the time in minutes that the user can be inactive before the session is disconnected. The default value is 15 minutes. A value of zero (0) indicates that the user is always active before the session is disconnected.
- **Limit Login Session for Web Logins:** Click **On** to limit the time that the user can be logged into the security appliance through a web browser. Enter the time in minutes in the **Login Session Limit** field. The default value is 10 minutes. A value of zero (0) indicates that there is no limit for web login sessions.

- **Web Server SSL Certificate:** Choose a certificate to authenticate users who try to access the Configuration Utility through a web browser by using HTTPS. By default, the web authentication server uses the default certificate for authentication. You can choose an imported certificate for authentication. The web authentication server will restart to load the selected certificate.
- **Management:** Check the box to enable access the configuration utility via HTTP or HTTPS. HTTP is enabled by default.

  NOTE: Unchecking both boxes will disable access to the configuration utility.
- **Allow Address:** Choose whether to allow access to the configuration utility from **Any** IP address or from a particular address or address range. The default setting is Any.

STEP 4 Click **Save** to apply your settings.

Configuring Remote Administration

You can enable Remote Administration to allow an administrator to connect to the configuration utility from a different network than the local network (LAN) of the security appliance. You can allow connections through HTTPS (HTTP over SSL) and HTTP.

When this feature is enabled, a user can access the configuration utility by launching a web browser and entering the protocol, the WAN IP address of the security appliance, and the specified Listen Port Number, as shown in this example: `https://209.165.201.1:8080`

NOTE To locally or remotely access the Configuration Utility from a PC running Windows Server 2008 and Internet Explorer 9 by using the HTTP protocol, add the URL (such as http://192.168.75.1:80/login.htm) as a trusted site. To add a trusted site in Internet Explorer 9, you can first open the browser and go to the Tools > Internet Options > Security page, and then select the **Trusted sites** zone and add your URL as a trusted site.

STEP 1 Click **Device Management > Administration > Remote Administration**.

STEP 2 Specify the following information:

- **Remote Administration:** Click **On** to enable remote management by using HTTPS, or click **Off** to disable it. We recommend that you use HTTPS for secure remote management.

- **HTTPS Listen Port Number:** If you enable remote management by using HTTPS, enter the port number. By default, the listen port number for HTTPS is 8080.
- **HTTP:** Click **On** to enable remote management by using HTTP, or click **Off** to disable it.
- **HTTP Listen Port Number:** If you enable remote management by using HTTP, enter the port number. By default, the listen port number for HTTP is 80.
- **Allow Address:** To specify the devices that can access the configuration utility through the WAN interface, choose an Address Object or enter an address.
  - **Address Objects:** These objects represent known IP addresses and address ranges, such as the GUEST VLAN and the DHCP pool. For details about the listed Address Objects, see the Networking > Address Management page.
  - **Create new address:** Choose this option to enter an IP address or address range. In the pop-up window, enter a **Name** and specify the **Type** (Host or Range). For a single host, enter the IP address. For a range, enter the **Starting IP Address** and the **Ending IP Address**.
- **Remote SNMP:** Click **On** to enable SNMP for the remote connection, or click **Off** to disable SNMP. Enabling SNMP allows remote users to use SNMP to manage the security appliance from the WAN side.

STEP 3 Click **Save** to apply your settings.

Configuring Email Alert Settings

Use the Email Alert page to centrally configure how to send the alert emails to the operator or administrator for specific events or behaviors that may impact the performance, operation, and security of your security appliance, or for debugging purposes.

When this feature is enabled, an alert is sent under these three conditions:

- The Web URL categories are changed.
- The Security Services application server status is No Authentication because the server is offline.

- DNS resolution of the Security Services application server name fails because the server is offline.

STEP 1 Click **Device Management > Administration > Email Alert**.

STEP 2 In the **Email Server** area, specify the SMTP email server that is used to send the alert emails.

- **SMTP Server:** Enter the IP address or Internet name of the SMTP server.
- **Port:** Enter the port for SMTP communication. The valid range of port numbers is 1~65535.
  - If you enter port 25 (the default setting), you can choose TLS (Transport Layer Security) or SSL (Secure Sockets Layer) for securing the SMTP communication, or choose None for an unsecured connection.
  - If you enter port 465, you can choose either TLS or SSL for securing the SMTP communication.
  - If you enter port 587, you can choose either TLS or SSL for securing the SMTP communication.
- **Secure Connectivity Method:** Choose either **TLS** or **SSL** for securing the SMTP communication, or choose **None** for an unsecured connection. If you choose TLS or SSL, SMTP Authentication will be enabled.
- **SMTP Authentication:** Click **On** if the SMTP server requires authentication before accepting the connections. Users must provide the SMTP account credentials for authentication.
- **Account:** Enter the username of the SMTP email account.
- **Password:** Enter the password of the SMTP email account.
- **From Email Address:** Enter the email address to send the alert emails.
- **To Email Address:** Enter the email address to receive the alert emails. This email address is used to receive all alert emails for all events. If you want to send the alert emails that belong to different events to different email addresses, uncheck **All Alerts** and then specify the email address for each event individually.

STEP 3 To verify the settings, click the **Test Connectivity to Email Server**. The results appear in a pop-up window.

STEP 4 In the **Event Alerts** area, specify the email alert settings for each event. When the relative events are detected, the alert emails are sent to the specified email address.

The following table provides information about how to enable the email alert feature for each event.

Event	Description
CPU Overload Alert	Sends an alert email if the CPU utilization is higher than the threshold over one minute and sends another alert email when the CPU utilization comes back down to normal for one minute. ▪ **CPU Threshold Setting:** Enter the value in the range 10% to 100% for CPU utilization threshold. The default value is 90%. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable CPU Overload Alert, you must complete the following tasks: ▪ Configure the email server settings used to send the alert emails. ▪ Check **CPU Overload Alert** in the **Enable** column and specify the CPU utilization threshold and the email address used to receive the alert emails.
New Firmware Alert	Sends an alert email to the specified email address if a newer firmware is detected on Cisco.com. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable New Firmware Alert, you must complete the following tasks: ▪ Configure the email server settings used to send the alert emails. ▪ Check **New Firmware Alert** in the **Enable** column and specify the email address used to receive the alert emails. **NOTE:** Make sure that you have an active WAN connection and a valid Cisco.com account to download the latest firmware image from Cisco.com and then install it on your security appliance. For complete details, see **Upgrading your Firmware from Cisco.com, page 436**.

Event	Description
License Expiration Alert	Sends an alert email a specified number of days before the security license expires. ▪ **days:** Enter the number of days before the license expires to send the alert email. The default value is 15 days. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable License Expiration Alert, you must complete the following tasks: ▪ Validate the security license on the security appliance in the Device Management > License Management page. See **Installing or Renewing Security License, page 441**. ▪ Configure the email server settings used to send the alert emails. ▪ Check **License Expiration Alert** in the **Enable** column, set the number of days before the license expires to send the alert emails, and specify the email address used to receive the alert emails.
Syslog Email	Sends the syslogs on schedule to the specified email address for troubleshooting purposes. ▪ **Send to Email Address:** Enter the email address to receive the syslog messages. To enable Syslog Email, you must complete the following tasks: ▪ Enable the Log feature and specify the subtitle in the syslog emails, the severity level of syslogs that you want to send, and the schedule when you want to send the syslogs in the Device Management > Logs > Log Settings page. See **Configuring Log Settings, page 444**. ▪ Enable the **Email Alert** feature for the facilities in the Device Management > Logs > Log Facilities page. The syslogs generated by the selected facilities can be sent to the specified email address. See **Configuring Log Facilities, page 447**. ▪ Configure the email server settings used to send the syslog messages. ▪ Check **Syslog Email** in the **Enable** column and specify the email address used to receive the syslog messages.

Event	Description
Site-to-Site VPN Up/Down Alert	Sends an alert email when a VPN tunnel is established, a VPN tunnel is down, or the VPN tunnel negotiation fails. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable Site-to-Site VPN Up/Down Alert, you must complete the following tasks: ▪ Enable the Site-to-Site VPN feature and specify the IPsec VPN policies used to establish the VPN tunnels in the VPN > Site-to-Site > IPsec Policies page. See Configuring a Site-to-Site VPN, page 340. ▪ Configure the email server settings used to send the alert emails. ▪ Check **Site-to-Site VPN Up/Down Alert** in the **Enable** column and specify the email address used to receive the alert emails.
WAN Up/Down Alert	Sends an alert email if the WAN link is up or down. ▪ **Alert Interval:** Specify how often, in minutes, that the security appliance sends the alert emails. Enter a value in the range 3 to 1440 minutes. The default value is 5 minutes. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable WAN Up/Down Alert, you must complete the following tasks: ▪ Configure the email server settings used to send the alert emails. ▪ Check **WAN Up/Down Alert** in the **Enable** column and specify the email address used to receive the alert emails.

Event	Description
Traffic Meter Alert	Sends an alert email when the traffic limit is reached, or before the traffic counter is reset. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable Traffic Meter Alert, you must complete the following tasks: ▪ Enable the Traffic Metering feature for both the primary WAN and the secondary WAN (if applicable) and specify the corresponding settings in the Networking > WAN > Traffic Metering pages. See Measuring and Limiting Traffic with the Traffic Meter, page 135. ▪ Configure the email server settings used to send the alert emails. ▪ Check **Traffic Meter Alert** in the **Enable** column and specify the email address used to receive the alert emails.
Anti-Virus Alert	Sends an alert email at the specified interval to a specified email address if viruses are detected. ▪ **Alert Interval:** Specify how often, in minutes, that the security appliance sends an alert email for virus events. Enter a value in the range 1 to 1440 minutes. The default value is 30 minutes. The security appliance will log the virus events between alert intervals and send them in an alert email to the specified email address. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable Anti-Virus Alert, you must complete the following tasks: ▪ Enable the Anti-Virus feature and specify the protocols to scan for viruses in the Security Services > Anti-Virus > General Settings page. See Configuring Anti-Virus, page 302. ▪ Configure the email server settings used to send the alert emails. ▪ Check **Anti-Virus Alert** in the **Enable** column, set the alert interval, and specify the email address used to receive the alert emails.

Event	Description
IPS Alert	Sends an alert email every 30 minutes to the specified email address if an attack is detected by the IPS service or if an application is blocked by the Application Control service. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable the IPS Alert feature, you must complete the following tasks: ▪ Enable IPS and configure the IPS settings. See Configuring Intrusion Prevention, page 321. ▪ Enable Application Control and configure the Application Control settings. See Configuring Application Control, page 309. ▪ Configure the email server settings used to send the alert emails. ▪ Check **IPS Alert** in the **Enable** column and specify the email address used to receive the alert emails.
Web URL Filtering Alert	Sends an alert email to the specified email address when Web URL categories have any changes. ▪ **Send to Email Address:** Enter the email address to receive the alert emails. To enable the Web URL Filtering Alert feature, you must complete the following tasks: ▪ Enable Web URL Filtering in the Security Services > Web URL Filtering > Policy to Zone Mapping page. See Configuring Web URL Filtering, page 327. ▪ Configure the email server settings used to send the alert emails. ▪ Check **Web URL Filtering Alert** in the **Enable** column and specify the email address used to receive the alert emails.

NOTE: If a global email address for receiving all alert emails is configured in the **To Email Address** field, it will be displayed in the **Send to Email Address** field for all categories.

STEP 5 Click **Save** to apply your settings.

Configuring SNMP

Simple Network Management Protocol (SNMP) is a network protocol used over User Datagram Protocol (UDP) that lets you monitor and manage the security appliance from a SNMP manager. SNMP provides a remote means to monitor and control the network devices, and to manage the configuration, statistics collection, performance, and security.

STEP 1 Click **Device Management > Administration > SNMP**.

STEP 2 Click **On** to enable SNMP, or click **Off** to disable SNMP. By default, SNMP is disabled.

STEP 3 If you enable SNMP, specify the SNMP version. The security appliance provides support for network monitoring using SNMP Versions 1, 2c, and 3. By default, SNMP Version 1 and 2 is selected.

STEP 4 After you enable SNMP and select the SNMP version, enter the following information:

- **System Contact:** Enter the name of the contact person for your security appliance.
- **Device:** Enter the device name for easy identification of your security appliance.
- **System Location:** Enter the physical location of your security appliance.
- **Security User Name:** Enter the name of the administrator account with the ability to access and manage the SNMP MIB objects. This is only available for SNMPv3.
- **Authentication Password:** Enter the password of the administrator account for authentication (the minimum length of password is 8 characters). This is only available for SNMPv3.
- **Encrypted Password:** Enter the password for data encryption (the minimum length of password is 8 characters). This is only available for SNMPv3.
- **SNMP Engine ID:** The engine ID of the SNMP entity. The engine ID is used as a unique identification between two SNMP entities. This is only available for SNMPv3.

STEP 5 To enable SNMP Trap, enter the following information:

- **SNMP Read-Only Community:** Enter the read-only community used to access the SNMP entity.

- **SNMP Read-Write Community:** Enter the read-write community used to access the SNMP entity.
- **Trap Community:** Enter the community that the remote trap receiver host receives the traps or notifications sent by the SNMP entity.
- **SNMP Trusted Host:** Enter the IP address or domain name of the host trusted by the SNMP entity. The trusted host can access the SNMP entity. Entering 0.0.0.0 in this field allows any host to access the SNMP entity.
- **Trap Receiver Host:** Enter the IP address or domain name of the remote host that is used to receive the SNMP traps.

STEP 6 Click **Save** to apply your settings.

Backing Up and Restoring a Configuration

Use the Device Management > Backup/Restore page to manage your configuration.

You can back up your current settings as a configuration file to your local PC or to a USB device if applicable. You can later restore the saved configuration if needed. You should always back up your configuration whenever you make any modifications to the device configuration or performing any firmware updates.

NOTE When saving the configuration to a file, the security license and self-signed certificates are not saved in the configuration file.

STEP 1 Click **Device Management > Backup/Restore**.

STEP 2 To back up the current settings to your local PC, perform the following steps:

a. In **Configuration Backup** area, select the **Save Configuration to PC** radio button and click **Backup**. The Encryption window opens.

b. If you want to encrypt the configuration, check **Encrypt** and enter the password in the **Key** field, and then click **OK**. Locate where you want to save the configuration file (configure.bin) and click **Save**.

c. If you do not want to encrypt the configuration, click **OK**. Locate where you want to save the configuration file (configure.xml) and click **Save**.

STEP 3 To back up the current settings on a USB device, perform the following steps:

a. Insert a USB device into the USB port on the back panel. Make sure that the USB Device Status shows "Device Attached." Click **Refresh** to refresh the status immediately.

b. In the **Configuration Backup** area, select the **Save Configuration to USB** radio button and click **Backup**. The Encryption window opens.

c. If you want to encrypt the configuration, check **Encrypt** and enter the password in the **Key** field, and then click **OK**. The current settings will be saved as a configuration file (configure.bin) to the USB device.

d. If you do not encrypt the configuration, click **OK**. The current settings will be saved as a configuration file (configure.xml) to the USB device.

NOTE: Set the password carefully and record it, otherwise you cannot upload the configuration file later without the correct password.

STEP 4 To restore the settings from a saved configuration file on your local PC, perform the following steps:

a. In **Configuration Restore** area, select the **Restore Configuration From PC** radio button.

b. Click **Browse** to select the saved configuration file from your local PC and click **Restore**.

c. If the selected configuration file is encrypted, the Encryption window opens. Enter the password in the **Key** field and click **OK**. The security appliance reboots with the saved settings of the selected configuration file.

STEP 5 To restore the settings from a saved configuration file on a USB device, perform the following steps:

a. Insert a USB device into the USB port on the back panel.

b. In the **Configuration Restore** area, select the **Restore Configuration from USB** radio button. Make sure that the USB Device Status shows "Device Attached." Click **Refresh** to refresh the status.

c. In the **Configuration files on USB device** area, all saved configuration files located on the USB device appear in the list. Select a configuration file and click **Restore**.

d. If the selected configuration file is encrypted, the Encryption window opens. Enter the password in the **Key** field and click **OK**. The security appliance reboots with the saved settings of the selected configuration file.

Managing Certificates for Authentication

Use the Certificate Management page to manage the certificates for authentication. You can perform the following tasks:

- View the certificate status and details. See **Viewing Certificate Status and Details, page 419**.
- To export a local certificate or a Certificate Signing Request (CSR) to your PC, check it and click the **Download** icon in the **Configure** column. See **Exporting Certificates to Your Local PC, page 420**.
- To export a local certificate or a CSR to a mounted USB device, check it and click the **Export to USB** icon in the **Configure** column. See **Exporting Certificates to a USB Device, page 421**.
- To import a CA certificate or a local certificate from your local PC, click **Import PC**. See **Importing Certificates from Your Local PC, page 421**.
- To import a CA certificate or a local certificate from a mounted USB device, click **Import USB**. See **Importing Certificates from a USB Device, page 422**.
- To generate a CSR, click **Request Signing**. See **Generating New Certificate Signing Requests, page 422**.
- To import a signed certificate for a CSR from your local PC, click the **Upload** icon in the **Configure** column. See **Importing Signed Certificate for CSR from Your Local PC, page 423**.
- To delete a certificate or a CSR, click the **Delete** (x) icon in the **Configure** column.
- To delete multiple certificates, check them and click **Delete**.

Viewing Certificate Status and Details

STEP 1 Click **Device Management > Certificate Management**.

The Certificate Management window opens. All existing certificates are listed in the table. The following certificate information is displayed:

- **Certificate:** The name of the certificate.
- **Type:** The type of the certificate. The security appliance supports three types of certificates:
  - **Certificate Signing Request:** A certificate request generated by your security appliance that needs to be sent to the Certificate Authority (CA) for signing. CSR contains all information required to create your digital certificate.
  - **Local Certificate:** The local certificate is issued by a trusted CA, and is involved in the applications like remote management and SSL VPN. To use a local certificate, you must first request a certificate from the CA and then import the certificate to your security appliance.
  - **CA Certificate:** The CA certificate is issued by intermediate certificate authorities, such as GoDaddy or VeriSign. The CA certificate is used to verify the validity of certificates generated and signed by the CA.

STEP 2 To view complete details for a certificate, click the **Detail** icon in the **Details** column.

Certificate Type	Details
CA Certificate or Local Certificate	▪ **Name:** Name used to identify this certificate. ▪ **Issuer:** Name of the CA that issued the certificate. ▪ **Subject:** Name which other organizations will see as the holder (owner) of this certificate. ▪ **Serial number:** Serial number maintained by the CA and used for identification purposes. ▪ **Valid from:** Date from which the certificate is valid. ▪ **Expires on:** Date on which the certificate expires. It is advisable to renew the certificate before it expires.
Certification Signing Request (CSR)	▪ **Name:** Name used to identify this CSR. ▪ **Subject:** Name which other organizations will see as the holder (owner) of this certificate.

Exporting Certificates to Your Local PC

You can export a local certificate or a CSR to your local PC. CA certificate is not allowed to export.

STEP 1 Click **Device Management > Certificate Management**.

STEP 2 To export a local certificate or a CSR to your local PC, click the **Download** icon in the **Configure** column.

- If you are downloading a CSR, the Download Certificate Signing Request window opens. Click **Download**. The certificate file will be saved in .pem format.

- If you are downloading a local certificate, the Download Certificate window opens. Enter a password in the **Enter Export Password** field to protect the certificate file and click **Download**. The certificate file will be saved in .p12 format.

Exporting Certificates to a USB Device

To export a local certificate or a CSR to a USB device, you must first insert the USB device into the USB port on the back panel. CA certificate is not allowed to export.

STEP 1 Click **Device Management > Certificate Management**.

STEP 2 To export a local certificate or a CSR to the USB device, click the **Export to USB** icon in the **Configure** column.

- If you are downloading a CSR, the Export Certificate Signing Request to USB window opens. Click **Export**. The CSR file will be saved on the USB device in .pem format.
- If you are downloading a local certificate, the Export Certificate to USB window opens. Enter a password in the **Enter Export Password** field to protect the certificate file and click **Export**. The certificate file will be saved on the USB device in .p12 format.

Importing Certificates from Your Local PC

You can import a local certificate or a CA certificate from your local PC.

STEP 1 Click **Device Management > Certificate Management**.

STEP 2 To import a local certificate or a CA certificate from your local PC, click **Import PC**.

STEP 3 Enter the following information:

- **Import a local end-user certificate with private key from a PKCS#12 (.p12) encoded file:** If you choose this option, click **Browse** to locate and select a local certificate file from your local PC, enter the certificate name in the **Certificate Name** field and the protection password in the **Import Password** field, and then click **Import**.

- **Import a CA certificate from a PEM (.pem or .crt) encoded file:** If you choose this option, click **Browse** to locate and select a CA certificate file from your local PC and click **Import**.

Importing Certificates from a USB Device

To import local or CA certificates from a USB device, you must first insert the USB device into the USB port on the back panel.

STEP 1 Click **Device Management > Certificate Management**.

STEP 2 To import a local certificate or a CA certificate from the USB device, click **Import USB**.

The Import Certificate window opens. All available local certificates and CA certificates appear in the list.

STEP 3 Check the certificate file, enter the certificate name in the **Certificate Name** field and the protection password in the **Import Password** field, and then click **Import**.

Generating New Certificate Signing Requests

STEP 1 Click **Device Management > Certificate Management**.

STEP 2 Click **Request Signing** to generate a new certificate signing request.

The Generate Certificate Signing Request window opens.

STEP 3 Enter the following information:

- **Certificate Alias:** Enter an alias name for the certificate.
- **Country Name:** Choose the country from the drop-down list.
- **State or Province Name:** Enter the state or province name of your location.
- **Locality Name:** Enter the address of your location.
- **Organization Name:** Enter your organization name.
- **Organization Unit Name:** Enter your department name.

- **Common Name:** Enter the common name for the certificate.
- **E-mail Address:** Enter your email address.
- **Subject Distinguished Name:** After you enter the above information, the Distinguished Name (DN) is created in this field.
- **Subject Key Type:** Displays the signature algorithm (RSA) used to sign the certificate. RSA is a public key cryptographic algorithm used for encrypting data.
- **Subject Key Size:** Choose the length of the signature: 502 bits, 1024 bits, or 2048 bits.

STEP 4 Click **Generate** to create a certificate signing request file.

After you generate a certificate signing request file, you need to export this file to your local PC for submission to a Registration or CA. The CSR file will be saved in .pem format.

Importing Signed Certificate for CSR from Your Local PC

You can upload the signed certificate for a CSR from your local PC.

STEP 1 Click **Device Management > Certificate Management**.

STEP 2 To import the signed certificate for a CSR from your local PC, click the **Upload** icon in the **Configure** column.

STEP 3 Click **Browse** to locate and select the signed certificate file for the CSR from your local PC, and then click **Upload**.

NOTE: The signed certificate file should be PEM (.pem or .crt) encoded.

Configuring Cisco Services and Support Settings

This section describes how to configure your Cisco.com account on the security appliance, enable or disable Cisco OnPlus, configure the remote support settings, and send the contents for system diagnosis. Refer to the following topics:

- **Configuring Cisco.com Account, page 424**
- **Configuring Cisco OnPlus, page 425**
- **Configuring Remote Support Settings, page 426**
- **Sending Contents for System Diagnosis, page 426**

Configuring Cisco.com Account

Use the Cisco.com Account page to configure your Cisco.com account credentials on the security appliance.

A valid Cisco.com account is required to download the latest firmware image from Cisco.com and to check for signature updates from Cisco's signature server for IPS, Application Control, and Anti-Virus. If you do not have one, go to https://tools.cisco.com/RPF/register/register.do by clicking the **Create a Cisco.com Account** link on this page to register a Cisco.com account.

NOTE You can also configure your Cisco.com account credentials by using the Setup Wizard. See Configuring Cisco.com Account Credentials, page 37.

STEP 1 Click **Device Management > Cisco Services & Support > Cisco.com Account**.

The Cisco.com Account window opens.

STEP 2 Enter the following information:

- **User Name:** Enter the name of your Cisco.com account.
- **Password:** Enter the password of your Cisco.com account.

STEP 3 Click **Save** to apply your settings.

Configuring Cisco OnPlus

Use the Cisco OnPlus page to enable or disable Cisco OnPlus Advanced Security Service on the security appliance. Enabling Cisco OnPlus Advanced Security Service allows your security appliance to send security reporting and notification data through the OnPlus Service. If an OnPlus appliance is not present in your network, this setting will have no effect.

For example, you can back up and restore the configuration, upgrade the firmware, and view the network usage reports, WAN bandwidth reports, and device utilization of the security appliance through the OnPlus Service. The security appliance can initiate or accept HTTP or HTTPS connection with the agent.

To learn more information about Cisco OnPlus, go to www.cisco.com/go/onplus.

STEP 1 Click **Device Management > Cisco Services & Support > Cisco OnPlus**.

STEP 2 Check the box next to **Enable Cisco OnPlus Advanced Security Service** to enable Cisco OnPlus on your security appliance, or uncheck this box to disable it. By default, Cisco OnPlus is enabled. This setting is provided mainly for support and troubleshooting purposes. If you disable Cisco OnPlus on the security appliance, Cisco OnPlus Service will be unable to communicate with the security appliance and overall management, monitoring, and reporting will be impacted.

NOTE: The security appliance only starts collecting the session data when the OnPlus appliance is connected.

STEP 3 If Cisco OnPlus is enabled, we recommend that you enable the following discovery protocols on your security appliance for optimal device discovery and topology support via the OnPlus portal:

- **Cisco Discovery Protocol (CDP):** Shows if CDP is enabled or disabled. You can click the link to view or edit its settings. See **CDP Discovery, page 432**.
- **Bonjour Discovery Protocol:** Shows if Bonjour is enabled or disabled. You can click the link to view or edit its settings. See **Bonjour Discovery, page 432**.

STEP 4 Click **Save** to apply your settings.

Configuring Remote Support Settings

Use the Remote Support page to enable the SSHv2 server for debugging purposes. This feature allows the engineers to use a unique console root password to log in to the security appliance for debugging operations.

STEP 1 Click **Device Management > Cisco Services & Support > Remote Support**.

STEP 2 Enter the following information:

- **SSHv2 Server:** Click **On** to enable the SSHv2 server for debugging, or click **Off** to disable it.
- **Remote Support Password:** Enter the root password for remote support in this field. The root password expires in 24 hours, so you must request for a new password after it expires.

STEP 3 Click **Save** to apply your settings.

Sending Contents for System Diagnosis

Use the Send Diagnostics page to select the contents like the configuration file, the syslog file, and the system status data and compress them into one file in zip format, and then send the compressed file to the specified email address for system diagnosis. You can set a password to protect the compressed file for security purposes.

STEP 1 Click **Device Management > Cisco Services& Support > Send Diagnostics**.

STEP 2 In the **Content (compressed)** area, choose the contents that you want to use for diagnosing the system. The selected files are compressed into one file.

- **Configuration File:** Click **On** to compress the configuration for system diagnosis.
- **Syslog File:** Click **On** to compress the syslog messages for system diagnosis.
- **System Status:** Click **On** to compress the system status data for system diagnosis.

STEP 3 In the **Password Protection** area, you can set a password to secure the compressed file.

- **Password Protection:** Click **On** to enable the password protection, or click **Off** to disable it.
- **Password:** If you enable the password protection, enter the password in this field.

STEP 4 In the **Email** area, specify the email address to receive the compressed file.

- You can send the compressed file to the email address specified on the Email Alert page by selecting the first radio button.
- If you want to temporarily send the compressed file to a specific email address for system diagnosis without changing the email address settings on the Email Alert page, select the **Other Address** radio button and enter the email address in the field.

STEP 5 Click **Save** to apply your settings.

STEP 6 Click **Send Now** to send the compressed file to the specified email address immediately.

STEP 7 Click **Download** to save the compressed file to your local PC.

Configuring System Time

Use the Date and Time page to manually configure the system time, or to dynamically synchronize the system time with the Network Time Protocol (NTP) server.

STEP 1 Click **Device Management > Date and Time**.

STEP 2 Specify the time zone from the **Time zone** drop-down list.

STEP 3 Select the **Manually Set System Time** radio button to manually set the date and time. Enter the values in the **Date** and **Time** fields.

STEP 4 Select the **Dynamically Set System Time** radio button to automatically synchronize the date and time with the specified NTP server:

- **Daylight Saving Time Adjustment:** Click **On** to automatically adjust the time for Daylight Saving Time, or click **Off** to disable it.
- **Default NTP Servers:** Click this option to use the default NTP server.

- **Custom NTP Servers:** Click this option to use a custom NTP server. Enter the IP addresses or domain names of up to two custom NTP servers in the **Server 1 Name/IP Address** and **Server 2 Name/IP Address** fields. The server 1 is the primary NTP server and the server 2 is the secondary NTP server.
- **Current Time:** Displays the current date and time synchronized with the configured NTP server.

STEP 5 Click **Save** to apply your settings.

Configuring Device Properties

Use the Device Properties page to configure the host name and domain name to identify your security appliance on the network.

STEP 1 Click **Device Management > Device Properties**.

STEP 2 Enter the following information:

- **Host Name:** Enter the host name for your security appliance, which is displayed on the network to identify your device.
- **Domain Name:** Enter a unique domain name to identify your network.

STEP 3 Click **Save** to apply your settings.

Diagnostic Utilities

Use the following diagnostic utilities to access configuration of the security appliance and to monitor the overall network health.

- **Ping, page 429**
- **Traceroute, page 429**
- **DNS Lookup, page 430**
- **Packet Capture, page 430**

NOTE These features require an active WAN connection.

Ping

Use the Ping page to test the connectivity between the security appliance and a connected device on the network.

STEP 1 Click **Device Management > Diagnostic Utilities > Ping**.

The Ping window opens.

STEP 2 Enter the following information:

- **IP Address or URL:** Enter the IP address or URL to ping.
- **Packet Size:** Enter the packet size in the range 32 to 65500 bytes to ping. The security appliance will send the packet with the specified size to the destination.
- **Number of Pings:** Enter the times to ping. The security appliance will send the packet for specific times to check the connectivity with the destination.

STEP 3 Click **Start** to ping the IP address or the URL, or click **Stop** to stop pinging.

Traceroute

Use the Traceroute page to view the route between the security appliance and a destination.

STEP 1 Click **Device Management > Diagnostic Utilities > Traceroute**.

The Traceroute window opens.

STEP 2 Enter the following information:

- **IP Address or URL:** Enter the IP address or URL of the destination.
- **Maximum Number of Hops:** Choose the maximum hop number.

STEP 3 Click **Start** to trace the route of the IP address or URL, or click **Stop** to stop tracing.

DNS Lookup

Use the DNS Lookup page to retrieve the IP address of any server on the Internet.

STEP 1 Click **Device Management > Diagnostic Utilities > DNS Lookup**.

STEP 2 Enter the IP address or domain name that you want to look up in the **IP Address or Domain Name** field.

STEP 3 Click **Run** to query the server on the Internet. If the host or domain name exists, you will see a response with the IP address.

STEP 4 Click **Clear** to clean up the querying results.

Packet Capture

Use the Packet Capture page to capture all packets that pass through a selected interface.

STEP 1 Click **Device Management > Diagnostic Utilities > Packet Capture**.

STEP 2 Choose an interface or a network (such as DEFAULT VLAN) that you want to capture the packets from the **Network** drop-down list.

NOTE: Selecting WAN1 or WAN2 (if applicable) means capturing the packets through a logical interface. Selecting GEx means capturing the packets through a physical interface. If you choose a VLAN, only inter-VLAN traffic will be captured.

STEP 3 Click **Start** to start capturing the packets, click **Stop** to stop capturing, or click **Save** to save the captured packets.

Device Discovery Protocols

The security appliance supports the following protocols to discover the devices:

- **UPnP Discovery, page 431**
- **Bonjour Discovery, page 432**
- **CDP Discovery, page 432**

- LLDP Discovery, page 433

UPnP Discovery

UPnP (Universal Plug and Play) allows for automatic discovery of devices that can communicate with your security appliance. The UPnP Portmaps table displays the port mapping entries of the UPnP-enabled devices that accessed your security appliance.

STEP 1 Click **Device Management > Discovery Protocols > UPnP**.

STEP 2 Enter the following information:

- **Universal Plug-n-Play (UPnP):** Click **On** to enable UPnP, or click **Off** to disable UPnP. If UPnP is disabled, the security appliance will not allow for automatic device configuration.
- **LAN:** Choose an existing VLAN to which the UPnP information is broadcasted and listened on.
- **Advertisement Period:** Enter the value in seconds of how often the security appliance broadcasts its UPnP information to all devices within range. The default value is 1800 seconds.
- **Advertisement Time to Live:** Enter the value expressed in hops for each UPnP packet. This is the number of steps a packet is allowed to propagate before being discarded. Small values will limit the UPnP broadcast range. The default value is 4.

STEP 3 Click **Save** to apply your settings.

STEP 4 After you enable UPnP, the information in the UPnP Portmaps table will be refreshed immediately. Click **Refresh** to manually refresh the data.

Bonjour Discovery

Bonjour is a service advertisement and discovery protocol. Bonjour only advertises the default services configured on the security appliance when Bonjour is enabled.

STEP 1 Click **Device Management > Discovery Protocols > Bonjour**.

STEP 2 Click **On** to enable Bonjour, or click **Off** to disable it. If you enable Bonjour, all default services such as CSCO-SB, HTTP, and HTTPS are enabled. You cannot disable a particular service. You can either enable Bonjour or disable it.

STEP 3 In the **VLAN Association** area, you can associate the VLANs for the default services. The default services will only be visible to the hosts that belong to the associated VLANs. By default, DEFAULT VLAN is the broadcasting domain.

- To associate a VLAN, choose a VLAN from the **VLAN** drop-down list and click **Apply**.
- To dissociate the VLANs from the default services, check the boxes next to the appropriate VLANs and click **Delete**.

STEP 4 Click **Save** to apply your settings.

CDP Discovery

Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco manufactured equipment. Each CDP enabled device sends periodic messages to a multicast address and also listens to the periodic messages sent by others in order to learn about neighboring devices and determine the status of these devices. See CDP Discovery, page 432.

STEP 1 Click **Device Management > Discovery Protocols > CDP**.

STEP 2 In the **CDP Configuration** area, enter the following information:

- **Cisco Discovery Protocol (CDP):** Control whether CDP will run on some, all, or none of Ethernet interfaces. Choose one of the following options:
  - **Enable All:** Enable CDP on all ports supported by the security appliance.
  - **Disable All:** Disable CDP on all ports.

  - **Per Port:** Configure CDP on selective ports. CDP per port is recommended.

- **CDP Timer:** Enter the value of the time interval between two successive CDP packets sent by the security appliance. The default value is 60 seconds.
- **CDP Hold Timer:** The hold timer is the amount of time the information sent in the CDP packet should be cached by the security appliance that receives the CDP packet, after which the information is expired. The default value is 180 seconds.

Note: The Voice VLAN ID is a read-only field. You can configure the Voice VLAN on the Networking > VLAN page. For more information, see Configuring a VLAN, page 137.

STEP 3 In the **Enable CDP** area, specify which interfaces will run CDP. Click **On** to enable CDP on an interface, or click **Off** to disable CDP. This is required if you choose **Per Port** from the **CDP** drop-down list.

STEP 4 Click **Save** to apply your settings.

LLDP Discovery

Link Layer Discovery Protocol (LLDP) enables network managers to troubleshoot and enhance network management by discovering and maintaining network topologies over multi-vendor environments. LLDP discovers network neighbors by standardizing methods for network devices to advertise themselves to other systems, and to store discovered information.

LLDP enables a device to advertise its identification, configuration, and capabilities to neighboring devices that store the data in a Management Information Base (MIB). The network management system models the topology of the network by querying these MIB databases.

STEP 1 Click **Device Management > Discovery Protocols > LLDP**.

STEP 2 Click **On** to enable LLDP, or click **Off** to disable it. If you enable LLDP, the LLDP neighbors appear in the LLDP Neighbors table.

STEP 3 To view the detail of a LLDP neighbor, check it and click **Details**.

STEP 4 To refresh the data in the LLDP Neighbors table, click **Refresh**.

STEP 5 Click **Save** to apply your settings.

Firmware Management

You can perform the following tasks to maintain the firmware:

- View the firmware status. See **Viewing Firmware Information, page 435**.
- Switch to the secondary firmware through the Configuration Utility. See **Using the Secondary Firmware, page 435**.
- Upgrade your firmware to the latest version from Cisco.com. See **Upgrading your Firmware from Cisco.com, page 436**.
- Upgrade your firmware from a firmware image on your local PC or on a USB device. See **Upgrading Firmware from a PC or a USB Device, page 437**.
- Automatically fall back to the secondary firmware. See **Firmware Auto Fall Back Mechanism, page 438**.
- Use the Rescue mode to recover the system. See **Using Rescue Mode to Recover the System, page 438**.

CAUTION During a firmware upgrade, do NOT close the browser window, navigate away from the upgrading page, turn off the device, shut down the PC, remove the cable, or interrupt the process in any way until the operation is complete. This process should take several minutes including the reboot process. Interrupting the upgrade process at specific points when the flash is being written to can corrupt the flash memory and render the security appliance unusable.

Viewing Firmware Information

STEP 1 Click **Device Management > Firmware**.

The Firmware window opens.

STEP 2 In the **Firmware Version** area, the following firmware information is displayed:

- **Primary Firmware Version:** The version of the primary firmware that you are using.
- **Secondary Firmware Version:** The version of the secondary firmware that you used previously.

Using the Secondary Firmware

If the primary firmware is not stable, you can manually set the secondary firmware that was in use as the primary firmware. The original primary firmware will then become the secondary firmware. We recommend that you back up your current settings for later use before you switch to the secondary firmware.

CAUTION Do not try to switch the firmware if a secondary firmware image is not present. Doing so can cause the security appliance to not boot up.

STEP 1 Click **Device Management > Firmware**.

The Firmware window opens.

STEP 2 In the **Firmware Version** area, click **Switch Firmware**.

A warning message appears saying “Preparing to reboot. Do you want to continue? WARNING: All current sessions will be closed and the system will be down for approximately 180 seconds.”

STEP 3 Click **Yes** to reboot the security appliance by using the secondary firmware image.

Upgrading your Firmware from Cisco.com

The security appliance automatically checks for firmware updates from Cisco.com every 24 hours. You can upgrade your firmware to the latest version if a newer firmware is available on Cisco.com. A valid Cisco.com account is required to download the firmware image from Cisco.com.

NOTE This feature requires an active WAN connection.

STEP 1 Click **Device Management > Firmware**.

The Firmware window opens.

STEP 2 In the **Upgrade Firmware** area, the following information will be displayed under the **Upgrade Firmware from Cisco.com** radio button:

- **Your firmware is up to date:** Displays this message if you are using the latest firmware. The **Upgrade Firmware from Cisco.com** radio button will be grayed out.
- **Last checked:** Displays the date and time for the last query.
- **Unable to check firmware status:** Displays this message if the security appliance cannot access Cisco's IDA server due to invalid WAN connection or any other reasons.
- **New Firmware Available:** Displays the version number of the latest firmware image on Cisco's IDA server if newer firmware is available after the query. The **Upgrade Firmware from Cisco.com** radio button will be activated.

STEP 3 If newer firmware is available on Cisco.com, select the **Upgrade Firmware from Cisco.com** radio button and then perform one of the following actions:

- To upgrade the firmware and keep using the current settings, click **Upgrade**.
- To upgrade the firmware and restore the factory default settings, click **Upgrade and Factory Reset**.

STEP 4 The Firmware Upgrade window opens. Follow the on-screen prompts to download and install the firmware on your security appliance. For complete details, see Upgrading your Firmware After your First Login, page 33.

Upgrading Firmware from a PC or a USB Device

This section describes how to manually upgrade the firmware from a firmware image on your local PC or on a USB device. You must first download the latest firmware image from Cisco.com and save it to your local PC or to a USB device.

STEP 1 Click **Device Management > Firmware**.

The Firmware window opens.

STEP 2 To manually upgrade the firmware from your local PC, perform the following steps:

a. In the **Upgrade Firmware** area, select the **Upgrade Firmware from PC** radio button.

b. Click **Browse** to locate and select the firmware image from your local PC.

c. To upgrade the firmware and keep using the current settings, click **Upgrade**.

d. To upgrade the firmware and restore the factory default settings, click **Upgrade and Factory Reset**.

STEP 3 To upgrade the firmware through a USB device, perform the following steps:

a. Insert the USB device with the firmware images into the USB port on the back panel.

b. In the **Upgrade Firmware** area, select the **Upgrade Firmware from USB** radio button. Make sure that the USB Device Status shows as “Device Attached.” Click **Refresh** to refresh the status.

c. In the **Firmware images on USB device** area, all firmware images located on the USB device appear in the list. Select a firmware image from the list to upgrade.

d. To upgrade the firmware and keep using the current settings, click **Upgrade**.

e. To upgrade the firmware and restore the factory default settings, click **Upgrade and Factory Reset**.

Firmware Auto Fall Back Mechanism

The security appliance includes two firmware images in the same NAND flash to provide an Auto Fall Back mechanism so that the security appliance can automatically switch to the secondary firmware when the primary firmware experiences a CRC error or cannot boot up successfully for five times.

- **CRC Error:** An error that the firmware cannot pass the CRC (Cyclic Redundancy Check) validation. Downloading an incomplete firmware or incompletely writing the firmware to the flash may cause the CRC error.
- **Boot Failure:** A failure that the firmware cannot boot up successfully for five times.

The Auto Fall Back mechanism operates as follows:

STEP 1 The security appliance first boots up with the primary firmware.

STEP 2 The bootloader checks the CRC for the primary firmware.

STEP 3 If the CRC error or the boot failure occurs for the primary firmware, the bootloader will switch to the secondary firmware.

STEP 4 The bootloader checks the CRC for the secondary firmware.

STEP 5 If the CRC error or the boot failure occurs for the secondary firmware, the Rescue mode starts up. In Rescue mode, the security appliance works as a TFTP server. You can use a TFTP client to upload the firmware image to upgrade the firmware. For more information about the Rescue mode, see **Using Rescue Mode to Recover the System, page 438**.

Using Rescue Mode to Recover the System

When the system has a booting problem, a device error occurs, or the system has a problem, the POWER/SYS light on the front panel is solid amber. Follow these steps to start up the Rescue mode directly and then recover the system.

STEP 1 Press and hold the **RESET** button on the back panel of the security appliance for more than 3 seconds and power the unit on simultaneously.

The Rescue mode starts up. The Status LED flashes green and then shines solid amber. In Rescue mode, the security appliance works as a TFTP server.

STEP 2 Remove all cables from the WAN and LAN ports.

STEP 3 Connect your PC to the LAN port.

STEP 4 Configure your PC with a static IP address of 192.168.75.100 and a subnet mask of 255.255.255.0.

STEP 5 On your PC, start your TFTP client, such as tftpd32. Specify the host IP address as 192.168.75.1 and transfer the ISA500 firmware file from your PC to the security appliance.

The security appliance will upgrade the firmware after you upload the image. This process should take several minutes including the reboot process.

IMPORTANT: During firmware upgrade, do not turn off the device, shut down the PC, interrupt the process, or remove the cable in any way until the operation is complete.

When the POWER/SYS light on the front panel is solid green, the system is operating normally.

Managing Security License

The security services are licensable. A valid security license is required to activate security services and to support SSLVPN with mobile devices such as smart phones and tablets. The Product Authorization Key (PAK) and a valid Cisco.com account are required to install the security license. You can find the license code from the paper license that is shipped with the unit.

Use the License Management page to manage the security license. Refer to the following topics:

- **Checking Security License Status, page 440**
- **Installing or Renewing Security License, page 441**

Checking Security License Status

You can view information for the security license, including the expiration date, the device credentials used to renew the license, and the email alert settings for license expiration events.

STEP 1 Click **Device Management > License Management**.

The License Management window opens. The following information is displayed.

- **Feature:** The name of the security license.
- **Status:** Shows if the security license is installed or not installed. The security license cannot be transferred or revoked once it is installed.
- **Expiration:** The date on which the security license expires.

STEP 2 Click **Credentials** to display the product ID and series number of the device and the device credentials. The device credentials may be requested by Cisco sales or support to complete or troubleshoot licensing.

STEP 3 Click **Email Alerts** to set up or view the email alert settings for license expiration events.

The Email Alerts window opens. The following information is displayed.

- **Email Alert:** Click **On** to enable email alerts for license expiration, or click **Off** to disable this feature.
- **From Email Address:** The email address to use as the sender of the alert emails.
- **Send to Email Address:** The email address where the alerts will be sent.
- **SMTP Server:** The IP address or Internet name of the SMTP server.
- **SMTP Authentication:** Click **On** to enable SMTP authentication, or click **Off** to disable this feature.
- **Alert when it is:** Enter a number to specify the time frame when the alert will be sent. For example, enter 14 to send the email two weeks before the license expires.

STEP 4 We recommend that you enable the License Expiration Alert feature so that the system can send an alert to remind you to renew the security license before it expires. Click the link on the page or go to the Device Management > Administration > Email Alert page to enable the License Expiration Alert feature

and configure the email server settings. See **Configuring Email Alert Settings, page 408**.

Installing or Renewing Security License

This section describes how to install the security license or renew the security license before it expires. A valid security license is required to activate security services and to support SSLVPN with mobile devices such as smart phones and tablets.

NOTE You can also validate the security license by using the Setup Wizard. See Validating Security License, page 39.

STEP 1 Contact your Cisco reseller to purchase a license. The series number, PID, and UDI of your device are required to apply for a license. You can find these information from the Status > Dashboard page or from the Device Management > License Management page.

STEP 2 Log in to the Configuration Utility.

STEP 3 Click **Device Management > License Management**.

STEP 4 To install the security license, click the **Install** icon. **Other option:** If the security license is installed, you can click the **Renew** icon to renew the security license before it expires. Choose the license type from the **License Type** drop-down list:

- **License Code (PAK) from Cisco.com:** Automatically retrieves and installs the license on the security appliance from the Cisco server. If you choose this option, enter the following information. These credentials are required for the security appliance to authenticate to the Cisco server.
  - **License Code:** Enter the license code (PAK).
  - **Cisco.com Login:** Enter the username of your Cisco.com account.
  - **Cisco.com Password:** Enter the password of your Cisco.com account.
  - **Email Address:** Enter the registered email address to receive the PAK.
- **License File download from Cisco.com:** Installs a security license that was previously downloaded to your PC. If you choose this option, click **Browse** to locate and select the license file from your PC.

  NOTE: Make sure that the security appliance is set to the current time, or the license will not install properly. See **Configuring System Time, page 427**.

STEP 5 Check the box of **Click here if you accept with SEULA** to accept the SEULA (Software End User License Agreement) requirements. You can click the **SEULA** link to see the detailed SEULA requirements on Cisco.com.

STEP 6 Click **Validate License** to validate the security license on your security appliance.

After the license is installed or renewed, the expiration date of the security license is updated immediately. The security services are activated by the security license.

Log Management

You can configure logs for various events that occur on your network. The event logs can be used for tracking potential security threats. A variety of events can be captured and logged for review. These logs can be saved to the local syslog daemon or to a specified remote syslog server, or be emailed to a specified email address.

This section describes how to view the event logs, and configure the log settings and the log facilities. Refer to the following topics:

- **Viewing Logs, page 442**
- **Configuring Log Settings, page 444**
- **Configuring Log Facilities, page 447**

Viewing Logs

Use the View Logs page to view the logs for specific severity level, log facility, or source and/or destination IP address, or to search the logs by keyword.

NOTE Make sure that you enable the Local Log feature before you view the logs. See **Configuring Log Settings, page 444**.

STEP 1 Click **Device Management > Logs > View Logs**.

STEP 2 Specify the logs to be viewed:

- **Log Severity:** Choose the severity level to filter the logs. For example: If you select Critical, all logs listed under the Critical, Emergency, and Alert categories are displayed.

- **Log Facility:** Choose the facility to filter the logs. All logs that belong to the selected facility and match the specified severity settings are displayed.
- **Keyword:** Enter the keyword to search the logs. All logs that contain the specified keyword are displayed.
- **Source IP Address:** Enter the source IP address to filter the firewall logs. All firewall logs that match this source IP address are displayed.
- **Destination IP Address:** Enter the destination IP address to filter the firewall logs. All firewall logs that match this destination IP address are displayed.

STEP 3 Click **Query**.

The query outputs appear in the **Logs** table. The following information is displayed.

- **Date:** The date of the event.
- **Severity:** The severity level of the event.
- **Facility:** The type of facility for the log.
- **Log Data:** A brief description for the event.
- **Source IP Address:** The source IP address for the firewall event.
- **Destination IP Address:** The source IP address for the firewall event.

STEP 4 You can optionally perform the following actions:

- Sort the log entries. The logs can be sorted by clicking the column header. By default, the logs are sorted by date and time in descending sequence. For example, if you click **Severity**, the logs are sorted by the severity level in ascending sequence. Double click **Severity**, the logs are sorted by the severity level in descending sequence.
- Navigate the log entries. When viewing large numbers of logs, you can specify how many logs are displayed in the table per page, or you can navigate these logs by using the navigation buttons if one page cannot show all logs.
- Click **Clear** to clean up all logs that are saved in the local syslog daemon.
- Click **Refresh** to refresh the log data.
- Click **Export** to export the logs to a defined destination for debugging purposes.

Configuring Log Settings

Use the Log Settings page to enable the Log feature and configure the log settings. You can set the log buffer size, log all unicast traffic or broadcast traffic destined to your device for troubleshooting purposes, specify which syslogs to be mailed to a specified email address on schedule, and set the severity level of the events that are logged. If you have a remote syslog server support, you can save logs to the remote syslog server.

STEP 1 Click **Device Management > Logs > Log Settings**.

STEP 2 In the **Log Settings** area, enter the following information:

- **Log:** Click **On** to enable the Log feature, or click **Off** to disable it.
- **Log Buffer:** If you enable the Log feature, specify the size for the local log buffer. The default value is 409600 bytes.

  NOTE: After you enable the Log feature and set the log buffer size, specify the severity level of the events that you want to log. These logs will be saved to the local log daemon. See **Step 7**.

STEP 3 In the **System Logs** area, if you want to monitor the security appliance with more traffic data, you can choose to log all unicast traffic and/or all broadcast or multicast traffic directed to your security appliance for troubleshooting purposes. The logs for unicast traffic and broadcast or multicast traffic are at the Information severity level.

- **Unicast Traffic:** Click **On** to log all unicast packets directed to the security appliance. Unicast traffic for all facilities will be logged, regardless of internal or external traffic.
- **Broadcast/Multicast Traffic:** Click **On** to log all broadcast or multicast packets directed to the security appliance. Broadcast or multicast traffic for all facilities will be logged, regardless of internal or external traffic.

  If both are unselected, the security appliance only logs the events based on your facility settings. The log facilities are used to log some interest events, such as wireless clients are associated, packets are blocked by firewall rules, viruses are detected by the Anti-Virus service, and so forth.

STEP 4 In the **Email Server** area, specify which syslogs to be mailed to a specified email address on schedule.

- **Email Alert:** Shows if the Syslog Email feature is enabled or disabled.
- **From Email Address:** The email address used to send the logs.

- **To Email Address:** The email address used to receive the logs.
- **SMTP Server:** The IP address or Internet name of the SMTP server.
- **SMTP Authentication:** Shows if the SMTP authentication is enabled or disabled.

  NOTE: The above email server settings are read only. You must enable the Syslog Email feature and configure the email server settings to send the syslog messages to a specified email address. You can click the **Set Email Alert** link or go to the Device Management > Administration > Email Alert page to do this. See **Configuring Email Alert Settings, page 408**.
- **Mail Subtitle:** Enter the subtitle that is displayed in the email. For example, if you set the device name as the subtitle, the email recipient can recognize quickly what device the logs or alerts are coming from.
- **Severity:** Choose the severity level for the logs that you want to send.

Severity Level	Description
Emergency (level 0, highest severity)	System unusable.
Alert (level 1)	Immediate action needed.
Critical (level 2)	Critical conditions.
Error (level 3)	Error conditions.
Warning (level 4)	Warning conditions.
Notification (level 5)	Normal but significant conditions.
Information (level 6)	Informational messages only.
Debug (level 7, lowest severity)	Debugging messages.

For example: If you select Critical, all logs listed under the Critical, Emergency, and Alert categories are sent.

STEP 5 In the **Email Schedule** area, specify the schedule to send the logs.

- **Frequency:** Choose the period of time that you want to send the logs.
  - **Hourly:** Send the logs on an hourly basis.

  - **Daily:** Send the logs at a specific time of every day. If you choose this option, specify the time to send the logs in the **Time** field.
  - **Weekly:** Send the logs on a weekly basis. If you choose this option, specify the day of the week in the **Day** field and the time in the **Time** field.

- **Day:** If the logs are sent on a weekly basis, choose the day of the week
- **Time:** Choose the time of day when the logs should be sent.

STEP 6 In the **Remote Logs** area, specify how to save the logs to a remote syslog server.

- **Remote Logs:** Click **On** to save the logs to the specified remote syslog server, or click **Off** to disable it.
- **Syslog Server:** Enter the IP address or domain name of the remote syslog server that runs a syslog daemon.
- **Severity:** Choose the severity level of the logs that you want to save to the remote syslog server.

  For example: If you select Critical, the logs listed under the Critical, Emergency, and Alert categories are saved to the remote syslog server.

STEP 7 In the **Local Log** area, choose the severity level for the events that you want to log. The logs will be saved to the local syslog daemon.

For example: If you select Critical, all log messages listed under the Critical, Emergency, and Alert categories are saved to the local syslog daemon.

STEP 8 Click **Save** to apply your settings.

NOTE Next steps:

- To specify which system messages are logged based on the facility, go to the Log Facilities page. See **Configuring Log Facilities, page 447**.
- (Optional) To enable the Syslog Email feature and configure the email server settings to send the syslog messages to a specified email address, go to the Device Management > Administration > Email Alert page. See **Configuring Email Alert Settings, page 408**.

Configuring Log Facilities

Use the Log Facilities page to specify which system messages are logged based on the facility and determine where to save the syslogs and whether to send the syslogs to a specified email address on schedule.

NOTE Before you configure the log facilities, make sure that you enable the Log feature, set the log buffer size, and specify the Email Alert, Remote Log, and Local Log settings. See **Configuring Log Settings, page 444**.

STEP 1 Click **Device Management > Logs > Logs Facilities**.

The Log Facilities window opens. All supported facilities are listed in the table.

STEP 2 Specify the following information:

- **Email Alert:** Check **Email Alert** to enable the email alert settings for all facilities, or check the box for a facility to enable the email alert settings for the selected facility.

  The events that belong to the selected facilities and match the specified severity level for Syslog Email are logged and the recorded syslogs are sent to the specified email address on schedule.

- **Remote Log:** Check **Remote Log** to enable the remote log settings for all facilities, or check the box of a facility to enable the remote log settings for the selected facility.

  The events that belong to the selected facilities and match the specified severity level for Remote Logs are logged and the recorded syslogs are saved to the specified remote syslog server.

- **Local Log:** Check **Local Log** to enable the local log settings for all facilities, or check the box of a facility to enable the local log settings for the selected facility.

  The events that belong to the selected facilities and match the specified severity level for Local Log are logged and the recorded syslogs are saved to the local syslog daemon.

  NOTE: For information on configuring the Email Alert, Remote Log, and Local Log settings, see **Configuring Log Settings, page 444**.

STEP 3 Click **Save** to apply your settings.

Rebooting and Resetting the Device

Use the Reboot/Reset page to reboot the security appliance or restore the security appliance to the factory default settings (if necessary) from the Configuration Utility. Refer to the following topics:

- **Restoring the Factory Default Settings, page 448**
- **Rebooting the Security Appliance, page 449**

Restoring the Factory Default Settings

To restore the security appliance to the factory default settings, you can press and hold the **RESET** button on the back panel for more than 3 seconds, or perform the **Reset to Factory Defaults** operation from the Configuration Utility.

CAUTION The Reset To Factory Defaults operation will wipe out the current settings used on the security appliance (including the imported certificates). We recommend that you back up your current settings before restoring the factory default settings.

STEP 1 Click **Device Management > Reboot/Reset**.

The Reboot/Reset window opens.

STEP 2 In the **Reset Device** area, click **Reset to Factory Defaults**.

A warning message appears saying “Preparing to restore the factory default settings. Do you want to continue? WARNING: The current configuration will be overwritten.”

STEP 3 Click **Yes** to reboot the security appliance with the factory default settings.

Rebooting the Security Appliance

To reboot the security appliance, you can press and release the **RESET** button on the back panel for less than 3 seconds, or perform the **Reboot** operation from the Configuration Utility.

STEP 1 Click **Device Management > Reboot/Reset**.

The Reboot/Reset window opens.

STEP 2 In the **Reboot Device** area, click **Reboot**.

A warning message appears saying “Preparing to reboot. Do you want to continue? WARNING: All current sessions will be closed and the system will be down for approximately 180 seconds.”

STEP 3 Click **Yes** to reboot the security appliance.

Configuring Schedules

The schedule specifies when the firewall rule or the application control policy is active. For example, if you want a firewall rule only to work on the weekend, you can create a schedule called “Weekend” that is only active on Saturday and Sunday.

STEP 1 Click **Device Management > Schedules**.

The Schedules window opens.

STEP 2 To create a new schedule, click **Add**.

Other options: To edit an entry, click the **Edit** (pencil) icon. To delete an entry, click the **Delete** (x) icon. To delete multiple entries, check them and click **Delete**.

The Schedule - Add/Edit window opens.

STEP 3 Enter the following information:

- **Schedule Name:** Enter the name for the schedule.

- **Schedule Days:** Schedules the firewall rule or the application control policy on all days or on specific days.
  - **All Days:** Choose this option if you want to keep the firewall rule or the application control policy always on.
  - **Specific Days:** Choose this option and then check the days that you want to keep the firewall rule or the application control policy active.
- **Schedule Time:** Schedules the firewall rule or the application control policy on all days or at a specific time of day.
  - **All Days:** Choose this option if you want to keep the firewall rule or the application control policy always on.
  - **Specific Times:** Choose this option if you want to keep the firewall rule or the application control policy active at specific times. Specify the **Start Time** and **End Time** by entering the hour and minute and choosing either AM or PM.

STEP 4 Click **OK** to save your settings.

STEP 5 Click **Save** to apply your settings.

A

Troubleshooting

This chapter describes how to fix some common issues that you may encounter when using the security appliance. It includes the following sections:

- Internet Connection, page 453
- Date and Time, page 456
- Pinging to Test LAN Connectivity, page 457

Internet Connection

Symptom: You cannot access the Configuration Utility from a PC on your LAN.

Recommended Actions:

STEP 1 Check the Ethernet connection between the PC and the security appliance.

STEP 2 Ensure that the IP address of your PC is on the same subnet as the security appliance. If you are using the recommended addressing scheme, your PC's address should be in the range 192.168.75.100 to 192.168.75.200.

STEP 3 Check the IP address of your PC. If the PC cannot reach a DHCP server, some versions of Windows and MacOS generate and assign an IP address. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the security appliance and reboot your PC.

STEP 4 If your IP address has changed and you don't know what it is, reset the security appliance to the factory default settings.

If you do not want to reset to factory-default settings and lose your configuration, reboot the security appliance and use a packet sniffer (such as Ethereal™) to capture packets sent during the reboot. Look at the ARP packets to locate the LAN interface address.

STEP 5 Launch your web browser and ensure that Java, JavaScript, or ActiveX is enabled. If you are using Internet Explorer, click **Refresh** to ensure that the Java applet is loaded. Close the browser and launch it again.

STEP 6 Ensure that you are using the correct login information. The factory default login name is cisco and the password is cisco. Ensure that CAPS LOCK is off when entering this information.

Symptom: The security appliance does not save my configuration changes.

Recommended Actions:

STEP 1 When entering configuration settings, click **OK** or **Save** before moving to another page or tab; otherwise your changes are lost.

STEP 2 Click **Refresh** or **Reload** in the browser, which will clear a cached copy of the old configuration.

Symptom: The security appliance cannot access the Internet.

Possible Cause: If you use dynamic IP addresses, your security appliance is not requesting an IP address from the ISP.

Recommended Actions:

STEP 1 Launch your browser and determine if you can connect to an external site such as www.cisco.com.

STEP 2 Launch the Configuration Utility and login.

STEP 3 Click **Status > Dashboard**.

STEP 4 In the **WAN Interface(s)** area, find the WAN1 Address. If 0.0.0.0 is shown, your security appliance has not obtained an IP address from your ISP. See the next symptom.

Symptom: The security appliance cannot obtain an IP address from the ISP.

Recommended Actions:

STEP 1 Turn off power to the cable or DSL modem.

STEP 2 Power off the security appliance.

STEP 3 Then reapply power to the cable or DSL modem.

STEP 4 When the modem lights indicate that it has resynchronized with the ISP, reapply power to the security appliance. If the security appliance still cannot obtain an ISP address, see the next symptom.

Symptom: The security appliance still cannot obtain an IP address from the ISP.

Recommended Actions:

STEP 1 Click **Networking > WAN > WAN Settings**.

STEP 2 Click the **Edit** (pencil) icon to configure the primary WAN port.

The WAN - Add/Edit window opens.

STEP 3 Ask your ISP the following questions:

- What type of network addressing mode is required for your Internet connection? In the **IPv4** tab, choose the correct ISP connection type in the **IP Address Assignment** drop-down list, and then enter the account information as specified by the ISP.
- Is your ISP expecting you to login from a particular Ethernet MAC address? If yes, in the **IPv4** tab, choose **Use the following MAC address** from the **MAC Address Source** drop-down list, and then enter the required MAC address in the **MAC Address** field.

Symptom: The security appliance can obtain an IP address, but PC is unable to load Internet pages.

Recommended Actions:

STEP 1 Ask your ISP for the addresses of its designated DNS servers. Configure your PC to recognize those addresses. For details, see your operating system documentation.

STEP 2 On your PC, configure the security appliance to be its TCP/IP gateway.

Date and Time

Symptom: Date shown is January 1, 2000.

Possible Cause: The security appliance has not yet successfully reached a Network Time Server (NTS).

Recommended Actions:

STEP 1 If you have just configured the security appliance, click **Device Management > Date and Time**.

STEP 2 Review the settings for the date and time.

STEP 3 Verify your Internet access settings.

Symptom: The time is off by one hour.

Possible Cause: The security appliance does not automatically adjust for Daylight Savings Time.

Recommended Actions:

STEP 1 Click **Device Management > Date and Time**.

STEP 2 Enable the **Daylight Saving Time Adjustment** feature.

STEP 3 Click **Save** to apply your settings.

Pinging to Test LAN Connectivity

The security appliance and most TCP/IP terminal devices contain a ping utility that sends an ICMP echo-request packet to the designated device. The device responds with an echo reply. Troubleshooting a TCP/IP network is made very easy by using the ping utility in your PC or workstation.

This section includes the following topics:

- **Testing the LAN Path from Your PC to Your Security Appliance, page 457**
- **Testing the LAN Path from Your PC to a Remote Device, page 458**

Testing the LAN Path from Your PC to Your Security Appliance

STEP 1 On your PC, click the Windows **Start** button, and then click **Run**.

STEP 2 Type ping <IP_address> where <IP_address> is the IP address of the security appliance. Example: ping 192.168.75.1.

STEP 3 Click **OK**.

STEP 4 Observe the display:

- If the path is working, you see this message sequence:
  ```
  Pinging <IP address> with 32 bytes of data
  Reply from <IP address>: bytes=32 time=NN ms TTL=xxx
  ```
- If the path is not working, you see this message sequence:
  ```
  Pinging <IP address> with 32 bytes of data
  Request timed out
  ```
- If the path is not working, check the physical connections between the PC and the security appliance. If the LAN port light is off, verify that the corresponding link lights are lit for your network interface card and for any hub ports that are connected to your workstation and security appliance.
- If the path is still not up, test the network configuration.
  - Verify that the Ethernet card driver software and TCP/IP software are installed and configured on the PC.

- Verify that the IP addresses for the security appliance and PC are correct and on the same subnet.

Testing the LAN Path from Your PC to a Remote Device

STEP 1 On your PC, click the Windows **Start** button, and then click **Run**.

STEP 2 Type ping -n 10 <IP_address> where -n 10 specifies a maximum of 10 tries and <IP address> is the IP address of a remote device such as your ISP's DNS server. Example: ping -n 10 10.1.1.1.

STEP 3 Click **OK** and then observe the display (see the previous procedure).

STEP 4 If the path is not working, perform the following tasks:

- Check that the PC has the IP address of your security appliance is listed as the default gateway. (If the IP configuration of your PC is assigned by DHCP, this information is not visible in your PC's Network Control Panel.)
- Verify that the network (subnet) address of your PC is different from the network address of the remote device.
- Verify that the cable or DSL modem is connected and functioning.
- Call your ISP and go through the questions listed in **The security appliance cannot obtain an IP address from the ISP.**
- Ask your ISP if it rejects the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by allowing traffic from the MAC address of only your broadband modem. Some ISPs additionally restrict access to the MAC address of just a single PC connected to that modem. If this is the case, configure your security appliance to clone or spoof the MAC address from the authorized PC. See Configuring WAN Settings for Your Internet Connection, page 122.

B

Technical Specifications and Environmental Requirements

The following table lists the technical specifications and environmental requirements for the security appliance.

Feature	ISA550	ISA550W	ISA570	ISA570W
Physical Interfaces	2 x RJ-45 connectors for LAN ports 1 x RJ-45 connector for WAN port 4 x RJ-45 connectors for LAN, WAN or DMZ ports 1 x USB connector for USB 2.0 1 x Power switch	2 x RJ-45 connectors for LAN ports 1 x RJ-45 connector for WAN port 4 x RJ-45 connectors for LAN, WAN or DMZ ports 1 x USB connector for USB 2.0 1 x Power switch 2 x external antennas	4 x RJ-45 connectors for LAN ports 1 x RJ-45 connector for WAN port 5 x RJ-45 connectors for LAN, WAN or DMZ ports 1 x USB connector for USB 2.0 1 x Power switch	4 x RJ-45 connectors for LAN ports 1 x RJ-45 connector for WAN port 5 x RJ-45 connectors for LAN, WAN or DMZ ports 1 x USB connector for USB 2.0 1 x Power switch 2 x external antennas
Operating Temperature	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)
Storage Temperature	-4 to 158°F (-20 to 70°C)	-4 to 158°F (-20 to 70°C)	-4 to 158°F (-20 to 70°C)	-4 to 158°F (-20 to 70°C)

Feature	ISA550	ISA550W	ISA570	ISA570W
Operating Humidity	10 to 90 percent relative humidity, non-condensing	10 to 90 percent relative humidity, non-condensing	10 to 90 percent relative humidity, non-condensing	10 to 90 percent relative humidity, non-condensing
Storage Humidity	5 to 95 percent relative humidity, non-condensing	5 to 95 percent relative humidity, non-condensing	5 to 95 percent relative humidity, non-condensing	5 to 95 percent relative humidity, non-condensing
Internal Power Supply				
Voltage Range	Normal Voltage: 100 to 240 VAC Voltage Variation Range: 90 to 264 VAC	Normal Voltage: 100 to 240 VAC Voltage Variation Range: 90 to 264 VAC	Normal Voltage: 100 to 240 VAC Voltage Variation Range: 90 to 264 VAC	Normal Voltage: 100 to 240 VAC Voltage Variation Range: 90 to 264 VAC
Input Frequency Range	Normal Frequency: 50 to 60 Hz Frequency Variation Range: 47 Hz to 63 Hz	Normal Frequency: 50 to 60 Hz Frequency Variation Range: 47 Hz to 63 Hz	Normal Frequency: 50 to 60 Hz Frequency Variation Range: 47 Hz to 63 Hz	Normal Frequency: 50 to 60 Hz Frequency Variation Range: 47 Hz to 63 Hz
Output Voltage Regulation	11.4 V to 12.6 V	11.4 V to 12.6 V	11.4 V to 12.6 V	11.4 V to 12.6 V
Output Current	MAX 2.5 A	MAX 2.5 A	MAX 1.667 A	MAX 1.667 A
Physical Specifications				
Form Factor	1 RU, 19-inch rack-mountable	1 RU, 19-inch rack-mountable	1 RU, 19-inch rack-mountable	1 RU, 19-inch rack-mountable
Dimensions (H x W x D)	1.73 x 12.1 x 7.30 inches (44 x 308 x 185.5 mm)	1.73 x 12.1 x 7.30 inches (44 x 308 x 185.5 mm) Antennas add approximately 1.24 inches (31.6 mm) to depth.	1.73 x 12.1 x 7.30 inches (44 x 308 x 185.5 mm)	1.73 x 12.1 x 7.30 inches (44 x 308 x 185.5 mm) Antennas add approximately 1.24 inches (31.6 mm) to depth.
Weight (with Power Supply)	1.20 kg (3.22 lb)	1.26 kg (3.38 lb)	1.3 kg (3.48 lb)	1.36 kg (3.64 lb)

C

Factory Default Settings

This chapter describes the factory default settings for the primary features, and provides the lists of predefined service and address objects. It includes the following sections:

- Device Management, page 461
- User Management, page 463
- Networking, page 464
- Wireless, page 468
- VPN, page 469
- Security Services, page 471
- Firewall, page 471
- Reports, page 473
- Default Service Objects, page 474
- Default Address Objects, page 478

Device Management

Feature	Setting
Remote Administration	Disable
Remote management using HTTPS	Disable
Access type	All IP addresses
HTTPS listen port number	8080

Feature	Setting
Remote management using HTTP	Disable
HTTP listen port number	80
Remote SNMP	Disable
User Session Settings	
Inactivity timeout	15 minutes (0 to 1000 minutes)
Limit login session for web logins	Disable
Login session limit	10 minutes (0 to 1000 minutes)
SNMP	Disable
SNMP Versions	SNMP Version 1 and 2, SNMP Version 3
Maximum number of certificates	128
Remote Support	Disable
Cisco OnPlus	Enable
Send Diagnostics	Disable
Date and Time	Dynamically set system time
Daylight saving time adjustment	Disable
Default NTP servers	Enable
Host Name	“router” and first three bytes of the MAC address
UPnP	Disable
Bonjour	Enable
CDP	Disable
LLDP	Disable
Syslog Settings	Disable
Email Alert Settings	
CPU Overload Alert	Disable

Feature	Setting
CPU threshold setting	90% (10% to 100%)
New Firmware Alert	Disable
License Expiration Alert	Disable
Alert before the license expires	15 days
Syslog Email	Disable
Site-to-Site VPN Up/Down Alert	Disable
WAN Up/Down Alert	Disable
WAN Up/Down alert interval	5 minutes (3 to 1440 minutes)
Traffic Meter Alert	Disable
Anti-Virus Alert	Disable
Anti-Virus alert interval	30 minutes (1 to 1440 minutes)
IPS Alert	Disable
Web URL Filtering Alert	Disable

User Management

Feature	Setting
User Groups	
Default administrator user group	admin
Available services for user groups	Web Login, SSL VPN, IPsec Remote Access, and Captive Portal
Maximum number of user groups	50
Local Users	
Default administrator username	cisco

Feature	Setting
Default administrator password	cisco
Maximum number of local users	100
User Authentication Methods	Local Database (default) RADIUS RADIUS+Local Database LDAP LDAP+Local Database

Networking

Feature	Setting
IPv4 or IPv6 Routing	IPv4 only
WAN Interfaces	
Maximum number of WAN interfaces	2
WAN1-Physical Port	GE1
WAN1-IP Address Assignment	DHCP Client
WAN1-MTU	Auto
WAN1-MTU Value	1500
WAN1-DNS Server Source	Get Dynamically from ISP
WAN1-MAC Address Source	Use Default MAC address
WAN1-Zone Mapping	WAN
Network Addressing Modes	DHCP Client, L2TP, PPTP, PPPoE, and Static IP
Port Mirroring	Disable

Feature	Setting
Port-based Access Control	Disable
WAN Redundancy Operation Modes	Equal Load Balancing (default) Load Balancing Failover Routing Table
VLANs	
Maximum number of VLANs	16
DEFAULT VLAN	VID=1 IP Address=192.168.75.1 Subnet=255.255.255.0 Spanning Tree=Disable DHCP Mode=DHCP Server DHCP Pool=192.168.75.100 to 200 Lease Time=1 day Default Gateway=192.168.75.1 Mapped Zone=LAN

Feature	Setting
GUEST VLAN	VID=2 IP Address=192.168.25.1 Subnet=255.255.255.0 Spanning Tree=Disable DHCP Mode=DHCP Server DHCP Pool=192.168.25.100 to 200 Lease Time=1 day Default Gateway=192.168.25.1 Mapped Zone=GUEST
VOICE VLAN	VID=100 IP Address=10.1.1.2 Subnet=255.255.255.0 Spanning Tree=Enable Mapped Zone=VOICE DHCP Mode=Disable
Zones	
Maximum number of zones	32
Predefined zones	WAN, LAN, DMZ, VPN, GUEST, SSLVPN, VOICE
Routing	
Routing mode	Disable
Maximum number of Static Routing rules	150
Dynamic Routing (RIP)	Disable
Policy-Based Routing	Disable

Feature	Setting
Maximum number of Policy-Based Routing rules	100
WAN QoS	Disable
Maximum number of traffic selectors	256
Maximum number of WAN QoS policy profiles	32
Maximum number of traffic selectors associated with one WAN QoS policy profile	64
LAN QOS	Disable
WLAN QoS	Disable
Service Management	
Maximum number of service groups	64
Maximum number of services	150
Maximum number of services in one service group	64
Address Management	
Maximum number of address groups	64
Maximum number of addresses	150
Maximum number of addresses in one address group	100
Maximum number of DDNS profiles	16
VRRP	Disable
IGMP Proxy	Enable
IGMP Snooping	Enable
IGMP Version (Default)	IGMP Version 3

Wireless

Feature	Setting
Wireless Radio	Disable
Basic Radio Settings	
Wireless mode	802.11b/g/n mixed
Wireless channel	Auto
Bandwidth channel	Auto
Extension channel	Lower
U-APSD	Disable
SSID isolation (between SSIDs)	Disable
Default SSIDs (cisco-data, cisco-guest, cisco3, cisco4)	Disable
SSID broadcast	Enable
Station isolation (between clients)	Disable
Security mode	Open
Wi-Fi Multimedia (WMM)	Enable
Wireless MAC Filtering	Disable
Advanced Radio Settings	
Guard interval	Long (800 ns)
CTS protection mode	Auto
Beacon interval	100 ms (20 to 999 ms)
DTIM interval	1 ms (1 to 255 ms)
RTS threshold	2347 ms (1 to 2347 ms)
Fragmentation threshold	2346 ms (256 to 2346 ms)
Power output	100%

Feature	Setting
Wi-Fi Protected Setup (WPS)	Disable
Rogue AP Detection	Disable
Captive Portal	Disable
Session timeout	60 minutes (0 to 480 minutes)
Idle timeout	5 minutes (0 to 480 minutes)

VPN

Feature	Setting
Site-to-Site VPN	Disable
Maximum number of Site-to-Site VPN tunnels	100 for ISA570 and ISA570W 50 for ISA550 and ISA550W
IKE Policies	
Maximum number of IKE policies	16
DefaultIke, Hash	SHA1
DefaultIke, Authentication	Pre-shared Key
DefaultIke, D-H Group	Group 2
DefaultIke, Encryption	ESP_AES_256
DefaultIke, Lifetime	24 hours
Transform Policies	
Maximum number of transform policies	16
DefaultTrans, Integrity	ESP_SHA1_HMAC
DefaultTrans, Encryption	ESP_AES_256

Feature	Setting
IPsec Remote Access	Disable
Maximum number of group policies	16
Teleworker VPN Client	Disable
Maximum number of group policies	16
Auto initiation retry	Disable
Retry interval	120 seconds (120 to 1800 seconds)
Retry limit	0 (0 to 16)
SSL VPN	disable
Maximum number of group policies	32
Gateway interface	WAN1
Gateway port number	443
Certificate file	Default
Client address pool	192.168.200.0
Client netmask	255.255.255.0
Idle timeout	2100 seconds (60 to 86400 seconds)
Session timeout	0 seconds (0, 60 to 1209600 seconds)
Client DPD timeout	300 seconds (0 to 3600 seconds)
Gateway DPD timeout	300 seconds (0 to 3600 seconds)
Keep alive	30 seconds (0 to 600 seconds)
Lease duration	43200 seconds (600 to 1209600 seconds)
Max MTU	1406 bytes (256 to 1406 bytes)

Feature	Setting
Rekey method	SSL
Rekey interval	3600 seconds (0 to 43200 seconds)
L2TP Server	Disable
IPsec Passthrough	Enable
PPTP Passthrough	Enable
L2TP Passthrough	Enable

Security Services

Feature	Setting
Anti-Virus	Disable
Application Control	Disable
Spam Filter	Disable
Intrusion Prevention (IPS)	Disable
Web Reputation Filtering	Disable
Web URL Filtering	Disable
Network Reputation	Enable

Firewall

Features	Setting
Default Firewall Rules	Prevent all inbound traffic and allow all outbound traffic

Features	Setting
Maximum number of custom firewall rules	100
NAT	
Dynamic PAT	Enable
Maximum number of Static NAT rules	64
Maximum number of Port Forwarding rules	64
Maximum number of Port Triggering rules	15
Maximum number of Advanced NAT rules	32
Content Filtering	Disable
MAC Address Filtering	Disable
Maximum number of MAC Address Filtering rules	100
IP - MAC Binding	
Maximum number of IP - MAC Binding rules	100
Attack Protection	
Block Ping WAN Interface	Enable
Stealth Mode	Enable
Block TCP Flood	Enable
Block UDP Flood	Enable
Block ICMP Notification	Enable
Block Fragmented Packets	Disable
Block Multicast Packets	Enable

Features	Setting
SYN Flood Detect Rate	128 max/sec (0 to 65535)
Echo Storm	15 packets/sec (0 to 65535)
ICMP Flood	100 packets/sec (0 to 65535)
Session Limits	
Maximum number of connections	60000 (1000 to 60000)
TCP timeout	1200 seconds (5 to 3600 seconds)
UDP timeout	180 seconds (5 to 3600 seconds)
Application Level Gateway (ALG)	
SIP ALG	Enable
H.323 ALG	Enable

Reports

Feature	Setting
Bandwidth Usage Reports	
Bandwidth Usage Report by IP Address	Disable
Bandwidth Usage Report by Internet Service	Disable
Website Visits Report	Disable
WAN Bandwidth Reports	Disable
Security Services Reports	
Anti-Virus Report	Disable
Application Control Report	Disable

Feature	Setting
Email Security Report	Disable
IPS Report	Disable
Network Reputation Report	Enable
Web Security Report	Disable

Default Service Objects

The following table displays all predefined service objects on the security appliance.

Service Name	Protocol	Port Start	Port End	Description
AIM-CONNECT	TCP	4443	4443	AOL Instant Messenger, direct connect
AIM-CHAT	TCP	5190	5190	AOL Instant Messenger, file transfer and chat
BGP	TCP	179	179	Border Gateway Protocol
BOOTP_client	UDP	68	68	Bootstrap Protocol
BOOTP_server	UDP	67	67	Bootstrap Protocol
CU-SEEME	TCP/UDP	7648	7652	Internet Videoconferencing Protocol
DHCP	UDP	67	67	Dynamic Host Configuration Protocol
DNS	TCP/UDP	53	53	Domain Name System
ESP	IP			Protocol 50
FINGER	TCP	79	79	Exchange of human-oriented status and user information

Service Name	Protocol	Port Start	Port End	Description
FTP-DATA	TCP	20	20	File Transfer Protocol, data transfer
FTP-CONTROL	TCP	21	21	File Transfer Protocol, control command
HTTP	TCP	80	80	HyperText Transfer Protocol
HTTPS	TCP	443	443	HTTP over SSL/TLS
ICMP Destination Unreachable	ICMP	3	0	
ICMP Ping Reply	ICMP	0	0	
ICMP Ping Request	ICMP	8	0	
ICMP Redirect Message	ICMP	5	0	
ICMP Router Advertisement	ICMP	9	0	
ICMP Router Solicitation	ICMP	10	0	
ICMP Source Quench	ICMP	4	0	
ICMP Time Exceeded	ICMP	11	0	
ICMP Timestamp	ICMP	13	0	
ICMP Type-6	ICMP	6	0	Alternate Host Address
ICMP Type-7	ICMP	7	0	Reserved
ICQ	TCP	5190	5190	Instant Messenger
IDENT	TCP	113	113	Authentication Service/Identification Protocol

Service Name	Protocol	Port Start	Port End	Description
IKE	UDP	500	500	IPsec Key Exchange
IMAP	TCP	143	143	Internet Message Access Protocol
IMAP2	TCP	143	143	Internet Message Access Protocol Version 2
IMAP3	TCP	220	220	Internet Message Access Protocol Version 3
IPSEC-UDP-ENCAP	UDP	4500	4500	IPsec over UDP
IRC	TCP	6660	6660	Internet Relay Chat, de facto port: 6660 to 6669
ISAKMP	UDP	500	500	
L2TP	UDP	1701	1701	Layer 2 Tunneling Protocol
NEWS	TCP	144	144	
NFS	UDP	2049	2049	Network File System
NNTP	TCP	119	119	Network News Transfer Protocol, NNTP over SSL uses the port 563
POP3	TCP	110	110	Post Office Protocol Version 3
PPTP	TCP	1723	1723	Microsoft Point-to-Point Tunneling Protocol
RCMD	TCP	512	512	
REAL-AUDIO	TCP	7070	7070	
REXEC	TCP	512	512	Remote Process Execution
RIP	UDP	520	520	Routing Information Protocol
RLOGIN	TCP	513	513	

Service Name	Protocol	Port Start	Port End	Description
RTELNET	TCP	107	107	Remote TELNET service
RTSP	TCP/UDP	554	554	Real Time Streaming Protocol
SFTP	TCP	115	115	Simple File Transfer Protocol
SHTTPD	TCP	8080	8080	Simple HTTPD
SHTTPDS	TCP	443	443	Simple HTTPD over SSL
SIP	TCP/UDP	5060	5060	Session Initiation Protocol
SMTP	TCP	25	25	Simple Mail Transfer Protocol
SNMP	TCP/UDP	161	161	Simple Network Management Protocol
SNMP-TRAPS	TCP/UDP	162	162	Simple Network Management Protocol - Trap
SQL-NET	TCP	1521	1521	
SSH	TCP/UDP	22	22	Secure Shell Protocol
STRMWORKS	UDP	1558	1558	
TACACS	TCP	49	49	Login Host Protocol
TELNET	TCP	23	23	
TELNET Secondary	TCP	8023	8023	
TELNET SSL	TCP	992	992	
TFTP	UDP	69	69	Trivial FTP
VDOLIVE	TCP	7000	7000	VDOLive Protocol

Default Address Objects

The following table displays all predefined address objects on the security appliance. The IP address, IP address and netmask, or IP range for these objects will be automatically modified depending on your configuration or network connection.

Address Name	Type	IP, IP/Netmask, or IP Range
WAN1_IP	Host	0.0.0.0
WAN1_GW	Host	0.0.0.0
WAN1_DNS1	Host	0.0.0.0
WAN1_DNS2	Host	0.0.0.0
WAN1_USER_DNS1	Host	0.0.0.0
WAN1_USER_DNS2	Host	0.0.0.0
WAN1_NETWORK	Network	0.0.0.0/255.255.255.255
WAN1_MAC	MAC	N/A
DEFAULT_IP	Host	192.168.75.1
DEFAULT_Network	Network	192.168.75.0/255.255.255.0
DEFAULT_DHCP_POOL	Range	192.168.75.100 to 192.168.75.200
GUEST_IP	Host	192.168.25.1
GUEST_Network	Network	192.168.25.0/255.255.255.0
GUEST_DHCP_POOL	Range	192.168.25.100 to 192.168.25.200
IPv4_Multicast	Range	224.0.0.0 to 239.255.255.255
SSLVPN_ADDRESS_POOL	Network	192.168.200.0/255.255.255.0

D

Where to Go From Here

Cisco provides a wide range of resources to help you and your customers obtain the full benefits of the Cisco ISA500 Series Integrated Security Appliances.

Product Resources	
Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Firmware Downloads	www.cisco.com/go/isa500software
Product Documentation	
Cisco ISA500 Series Integrated Security Appliances	www.cisco.com/go/isa500resources
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb